Installationshandbuch

Identity Manager 4.0.2

22. Juni 2012

Novell

Rechtliche Hinweise

Novell, Inc. übernimmt für Inhalt oder Verwendung dieser Dokumentation keine Haftung und schließt insbesondere jede ausdrückliche oder implizite Garantie für Marktfähigkeit oder Eignung für einen bestimmten Zweck aus. Novell, Inc. behält sich das Recht vor, dieses Dokument jederzeit teilweise oder vollständig zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen davon in Kenntnis zu setzen.

Novell, Inc. gibt ebenfalls keine Erklärungen oder Garantien in Bezug auf Novell-Software und schließt insbesondere jede ausdrückliche oder implizite Garantie für handelsübliche Qualität oder Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc. das Recht vor, Novell-Software jederzeit ganz oder teilweise zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen von diesen Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie erkennen alle Ausfuhrkontrollbestimmungen an und erklären sich damit einverstanden, alle für ausstehende Exporte, Re-Exporte oder Importe erforderlichen Lizenzen bzw. Klassifizierungen einzuholen. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen aufgeführte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden. Weitere Informationen zum Export von Novell-Software finden Sie auf der Webseite Novell International Trade Services (http://www.novell.com/info/exports/). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Copyright © 2007–2012 Novell, Inc. Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Herausgebers darf kein Teil dieser Veröffentlichung reproduziert, fotokopiert, übertragen oder in einem Speichersystem verarbeitet werden.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online-Dokumentation: Die neueste Online-Dokumentation für dieses und andere Novell-Produkte finden Sie auf der Dokumentations-Webseite von Novell (http://www.novell.com/documentation).

Novell-Marken

Hinweise zu Novell-Marken finden Sie in der Novell Trademark and Service Mark-Liste (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.

Inhalt

Informationen zu diesem Handbuch 7

Teil I Planung 9

1 Einrichten einer Entwicklungsumgebung 11

2 Erstellen eines Projektplans 13

2.1 Ermittlungsphase . . . 13
2.1.1 Definieren aktueller Geschäftsprozesse . . . 14
2.1.2 Definieren, wie sich die Identity Manager-Lösung auf die aktuellen Geschäftsprozesse auswirkt . . . 15
2.1.3 Identifizieren der wichtigsten Projektbeteiligten auf geschäftlicher und technischer Ebene . . . 16
2.1.4 Gespräche mit allen Projektbeteiligten führen . . . 16
2.1.5 Erstellen einer allgemeinen Strategie und eines konsensfähigen Ausführungsablaufs . . . 17
2.2 Anforderungs- und Entwurfsanalysephase . . . 17
2.2.1 Definieren der Geschäftsanforderungen . . . 18
2.2.2 Analysieren der Geschäftsprozesse . . . 20
2.2.3 Entwurf eines Enterprise-Datenmodells . . . 20
2.3 Proof-of-Concept . . . 22
2.4 Validierung und Vorbereitung der Daten . . . 22
2.5 Produktions-Prototyp . . . 23
2.6 Planung des Produktions-Rollout . . . 23
2.7 Produktionsbereitstellung . . . 24

3 Technische Richtlinien 25

3.1 Verwaltungswerkzeuge - Richtlinien . . . 26
3.1.1 Analyzer-Richtlinien . . . 27
3.1.2 Designer-Richtlinien . . . 27
3.1.3 iManager-Richtlinien . . . 27
3.1.4 Rollenzuordnungsadministrator-Richtlinien . . . 27
3.2 Metaverzeichnis-Server-Richtlinien . . . 28
3.3 eDirectory-Richtlinien . . . 29
3.3.1 Identity Manager-Objekte in eDirectory . . . 29
3.3.2 Reproduktion der von Identity Manager auf dem Server benötigten Objekte . . . 30
3.3.3 Verwendung der Bereichsfilterung zum Verwalten von Benutzern auf verschiedenen Servern . . . 31
3.4 Benutzeranwendung . . . 34
3.5 Revision und Berichterstellung - Richtlinien . . . 34

Teil II Installation 37

4 Basis-Checkliste für das Identity Manager-System 39

4.1 Voraussetzungen . . . 40
4.2 Planung . . . 40
4.3 Installation . . . 40

4.4 Treiberkonfiguration mit dem Remote Loader . . . 41
4.5 Treiberkonfiguration ohne den Remote Loader . . . 41
4.6 Zusätzliche Konfiguration . . . 42

5 Bezugsquellen für Identity Manager 43

6 Systemanforderungen 47

6.1 eDirectory und iManager . . . 50
6.2 Metaverzeichnis-Server . . . 51
6.2.1 Unterstützte Prozessoren . . . 52
6.2.2 Server-Betriebssysteme . . . 52
6.3 Remote Loader . . . 54
6.4 Benutzeranwendung . . . 57
6.5 Revision und Berichterstellung . . . 57
6.6 Arbeitsstationen . . . 59
6.6.1 Arbeitsstationsplattformen . . . 60
6.6.2 Webbrowser . . . 61
6.7 Ressourcenanforderungen . . . 61

7 Installation von Identity Manager 63

7.1 Installation von Analyzer . . . 63
7.2 Installation von Designer . . . 64
7.3 Installieren von eDirectory . . . 65
7.4 Installieren von iManager . . . 66
7.5 Installation des Metaverzeichnis-Servers . . . 66
7.5.1 Nicht-root-Installation des Metaverzeichnis-Servers . . . 68
7.5.2 Automatische Installation des Metaverzeichnis-Servers . . . 69
7.6 Installation des Remote Loaders . . . 70
7.6.1 Anforderungen . . . 71
7.6.2 Unterstützte Treiber . . . 71
7.6.3 Installationsvorgang . . . 72
7.6.4 Automatische Installation des Remote Loaders . . . 74
7.6.5 Installation des Java Remote Loader unter UNIX oder Linux . . . 74
7.6.6 Koexistenz von 32-Bit- und 64-Bit-Remote Loader . . . 75
7.7 Installation der Treiberdateien . . . 76
7.8 Installation des rollenbasierten Bereitstellungsmoduls . . . 77
7.9 Installation eines benutzerdefinierten Treibers . . . 77
7.10 Installation des Rollenzuordnungsadministrators . . . 77
7.11 Installation des Identitätsberichterstellungsmoduls der Sentinel-Anwendung . . . 78
7.12 Sprachunterstützung für die Identity Manager-Installationsprogramme . . . 78
7.12.1 Überlegungen zu Sprachen, die nicht von den Installationsprogrammen unterstützt werden . . . 80

8 Aktivieren von Novell Identity Manager-Produkten 81

8.1 Erwerb einer Produktlizenz für Identity Manager . . . 81
8.2 Installation einer Produktaktivierungsberechtigung . . . 82
8.3 Anzeigen der Produktaktivierungen für Identity Manager und Identity Manager-Treiber . . . 83
8.4 Aktivieren von Identity Manager-Treibern . . . 83
8.5 Aktivieren von Analyzer . . . 84
8.6 Aktivieren von Designer und dem Rollenzuordnungsadministrator . . . 84

9 Fehlerbehebung in Identity Manager 85

10 Neue Funktionen 93

10.1 Neuerungen in Identity Manager 4.0.2 . . . 93
10.1.1 Neue Treiber . . . 93
10.1.2 Funktionen für die Passwortverwaltung . . . 94
10.1.3 Funktionen für den Rollenzuordnungsadministrator . . . 94
10.1.4 Funktionen des rollenbasierten Provisioning-Moduls . . . 95
10.1.5 Funktionen für das Identitätsberichterstellungsmodul . . . 95
10.1.6 Designer-Funktionen . . . 96
10.1.7 Analyzer-Funktionen . . . 97
10.2 Neuerungen in Identity Manager 4.0.1 . . . 97
10.2.1 Identity Manager Advanced Edition im Vergleich zur Standard Edition . . . 97
10.2.2 Telemetrie . . . 98
10.2.3 Aktivität „Ressourcenanforderung“ . . . 98
10.2.4 Neue Berichte für das Identitätsberichterstellungsmodul . . . 98
10.2.5 Anwendungen, die zur Designer-Palette hinzugefügt wurden . . . 98
10.3 Neuerungen in Identity Manager 4.0 . . . 98
10.3.1 Identitätsberichterstellungsmodul . . . 99
10.3.2 Neue Treiber . . . 99
10.3.3 Unterstützung für XDAS-Revisionen . . . 100
10.3.4 Pakete ersetzen Treiberkonfigurationsdateien . . . 100
10.3.5 Rollenzuordnungsadministrator . . . 100
10.3.6 Analyzer . . . 100
10.3.7 Integriertes Installationsprogramm . . . 100

Teil III Aufrüsten von Identity Manager 101

11 Aufrüstung im Vergleich zu Migration 103

Teil IV Deinstallation von Identity Manager 105

12 Deinstallation der Identity Manager-Komponenten 107

12.1 Entfernen von Objekten aus eDirectory . . . 107
12.2 Deinstallation des Metaverzeichnis-Servers . . . 108
12.2.1 Deinstallation unter Linux/UNIX . . . 108
12.2.2 Deinstallieren einer Nicht-root-Installation . . . 108
12.2.3 Deinstallation unter Windows . . . 108
12.3 Deinstallieren von Remote Loader . . . 109
12.3.1 Deinstallation unter Linux/UNIX . . . 109
12.3.2 Deinstallation unter Windows . . . 109
12.4 Deinstallation des rollenbasierten Bereitstellungsmoduls . . . 109
12.4.1 Löschen der Treiber . . . 109
12.4.2 Deinstallation der Benutzeranwendung . . . 110
12.4.3 Deinstallation des Anwendungsservers und der Datenbank . . . 110
12.5 Deinstallation der Komponenten des Identitätsberichterstellungsmoduls . . . 111
12.5.1 Löschen der Berichterstellungstreiber . . . 111
12.5.2 Deinstallation des Identity-Berichterstellungsmoduls . . . 111
12.5.3 Deinstallation des Event Auditing Service . . . 112
12.6 Deinstallieren von iManager . . . 112
12.7 Deinstallieren von eDirectory . . . 112
12.8 Deinstallation von Analyzer . . . 114
12.9 Deinstallation von Designer . . . 114
12.10 Deinstallation des Rollenzuordnungsadministrators . . . 114

Informationen zu diesem Handbuch

Novell Identity Manager ist ein Service für die Datenfreigabe und -synchronisierung, mit dessen Hilfe Anwendungen, Verzeichnisse und Datenbanken Informationen gemeinsam nutzen können. Er verbindet über mehrere Verzeichnisse verstreute Informationen und ermöglicht Ihnen das Einrichten von Richtlinien für die automatische Aktualisierung designierter Systeme bei Identitätsänderungen. Identity Manager bietet die Grundlage für Kontenbereitstellung, Sicherheit, Single Sign-on, Benutzerselbstbedienung, Authentifizierung, Autorisierung, automatisierten Workflow und Webservices. Das Programm ermöglicht Ihnen, die verteilten Identitätsinformationen zu integrieren, zu verwalten und zu steuern, sodass Sie den richtigen Personen die richtigen Ressourcen auf sichere Weise zur Verfügung stellen können.

Dieses Handbuch enthält Informationen zur Planung, Installation oder zum Aufrüsten eines Identity Manager-Systems, das auf Ihre Umgebung zugeschnitten ist.

- Teil I, „Planung“, auf Seite 9
  - Kapitel 1, „Einrichten einer Entwicklungsumgebung“, auf Seite 11
  - Kapitel 2, „Erstellen eines Projektplans“, auf Seite 13
  - Kapitel 3, „Technische Richtlinien“, auf Seite 25
- Teil II, „Installation“, auf Seite 37
  - Kapitel 4, „Basis-Checkliste für das Identity Manager-System“, auf Seite 39
  - Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 43
  - Kapitel 6, „Systemanforderungen“, auf Seite 47
  - Kapitel 7, „Installation von Identity Manager“, auf Seite 63
  - Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 81
  - Kapitel 9, „Fehlerbehebung in Identity Manager“, auf Seite 85
  - Kapitel 10, „Neue Funktionen“, auf Seite 93
- Teil III, „Aufrüsten von Identity Manager“, auf Seite 101
  - Kapitel 11, „Aufrüstung im Vergleich zu Migration“, auf Seite 103
- Teil IV, „Deinstallation von Identity Manager“, auf Seite 105

Zielgruppe

Dieses Handbuch richtet sich an Administratoren, Berater und Netzwerkingenieure, die für die Planung und Implementierung von Identity Manager in einer Netzwerkumgebung zuständig sind.

Aktualisierungen der Dokumentation

Die neueste Version dieses Dokuments finden Sie auf der Website zur Identity Manager-Dokumentation (http://www.novell.com/documentation/idm402/index.html).

Zusätzliche Dokumentation

Zusätzliche Dokumentation zu Identity Manager-Treibern finden Sie auf der Website für Identity Manager-Treiberdokumentation (http://www.novell.com/documentation/idm402drivers/index.html).

Dokumentation zur Benutzeranwendung finden Sie auf der Website zur Novell-Dokumentation für das rollenbasierte Bereitstellungsmodul für Identity Manager (http://www.novell.com/documentation/idmrbpm402/index.html).

Planung

Identity Manager 4.0.2 unterstützt Sie bei der Verwaltung von Identitäten und Ressourcen in Ihrem Unternehmen. Darüber hinaus dient es zur Automatisierung vieler Geschäftsprozesse, die zurzeit noch manuell abgewickelt werden.

Weitere Informationen zu den einzelnen Komponenten, aus denen eine Identity Manager-Lösung besteht, finden Sie im *Identity Manager 4.0.2 Overview* (Identity Manager 4.0.1 Übersichtshandbuch).

Zum Erstellen einer effektiven Identity Manager-Lösung für Ihre Umgebung müssen Sie sich zunächst die Zeit nehmen, die Lösung zu planen und zu entwickeln. Die Planung beinhaltet zwei wesentliche Aspekte: die Einrichtung eines Testlabors, um sich mit den Produkten vertraut zu machen, und die Erstellung eines Projektplans, um eine Identity Manager-Lösung zu implementieren. Wenn Sie einen Projektplan erstellen, schließt dies die Definition Ihres Geschäftsprozesses und das Erstellen eines Implementierungsplans ein. In den meisten Unternehmen gibt es viele verschiedene Geschäftsprozesse, die von unterschiedlichen Personen verwaltet werden. Eine vollständige Identity Manager-Lösung wirkt sich auf die meisten dieser Prozesse aus. Es ist sehr wichtig, für die Planung einer Identity Manager-Lösung genügend Zeit einzuplanen, damit diese effektiv in Ihre Umgebung implementiert werden kann.

Wenn Sie eine neue Identity Manager-Lösung erstellen, in der sich alle Komponenten auf demselben Server befinden, ziehen Sie für die Installation das *Handbuch zur integrierten Installation von Identity Manager 4.0.2* zu Rate. Dieses beschreibt ein vereinfachtes Installationsverfahren, mit dem Sie das System schneller einrichten können.

Es wird empfohlen, in jeder Phase der Identity Manager-Implementierung einen Identity Manager-Spezialisten hinzuzuziehen. Weitere Informationen zu möglichen Partnerschaften finden Sie auf der Partner-Website von Novell (http://www.novell.com/partners/). Novell Education bietet auch Kurse für die Identity Manager-Implementierung an.

- Kapitel 1, „Einrichten einer Entwicklungsumgebung“, auf Seite 11
- Kapitel 2, „Erstellen eines Projektplans“, auf Seite 13
- Kapitel 3, „Technische Richtlinien“, auf Seite 25

1 Einrichten einer Entwicklungsumgebung

Bevor Sie die Planungsphase der Identity Manager-Bereitstellung beginnen, müssen Sie mit den Identity Manager-Produkten vertraut sein, damit Sie einen nützlichen Plan erstellen können. Wenn Sie eine Entwicklungsumgebung einrichten, in der Sie Ihre Identity Manager-Lösung entwickeln, analysieren und testen können, lernen Sie jede Komponente des Identity Manager kennen und stoßen dabei möglicherweise auf unerwartete Probleme.

Wenn Sie beispielsweise Informationen zwischen verschiedenen Systemen synchronisieren, werden dabei die Informationen für jedes System unterschiedlich präsentiert. Wenn Sie die zwischen zwei Systemen zu synchronisierenden Daten ändern, können Sie erkennen, ob sich diese Änderung auf andere Systeme auswirkt, die dieselben Informationen verwenden.

Ein anderer wesentlicher Grund für die Einrichtung einer Entwicklungsumgebung besteht darin, sicherzustellen, dass Ihre Lösungen funktionieren, bevor Sie sie auf „echte“ Daten anwenden. Identity Manager bearbeitet und löscht Daten. In einer Testumgebung können Sie Änderungen an Daten vornehmen, ohne dass die „echten“ Daten in Ihrer Produktionsumgebung davon betroffen sind.

Die sollten für jede Bereitstellung des Identity Manager eine Entwicklungsumgebung einrichten. Bereitstellungen unterscheiden sich voneinander. Es gibt unterschiedliche Systeme, Geschäftsrichtlinien und Prozeduren, die in der Identity Manager-Lösung berücksichtigt werden müssen. Eine Entwicklungsumgebung ermöglicht Ihnen, eine auf die jeweilige Situation zugeschnittene Lösung zu erarbeiten.

Das wichtigste Werkzeug beim Entwickeln Ihrer Identity Manager-Lösung ist Designer. Mit ihm können Sie alle Informationen zu Ihrer Umgebung erfassen und diese anschließend zum Erstellen einer individuell zugeschnittenen Identity Manager-Lösung verwenden. Sie sollten Designer zur Erfassung aller benötigten Informationen für alle Aspekte der Planung einsetzen. Designer vereinfacht das Erstellen eines Projektplans, der sowohl geschäftliche als auch technische Informationen umfasst. Weitere Informationen zu Designer finden Sie im *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide* (Administrationshandbuch zu Designer 4.0.1 für Identity Manager 4.0.1).

Verwenden Sie zum Einrichten Ihrer Entwicklungsumgebung die Informationen in Kapitel 4, „Basis-Checkliste für das Identity Manager-System“, auf Seite 39. Es handelt sich um eine Installations-Checkliste für alle Identity Manager-Komponenten. Stellen Sie anhand dieser Liste sicher, dass Sie alle Komponenten für Identity Manager, die Sie für die Erstellung eines Projektplans benötigen, installiert und konfiguriert haben. Die Informationen in Kapitel 3, „Technische Richtlinien“, auf Seite 25 sind hilfreich beim Einrichten Ihrer Entwicklungsumgebung. Sie erfahren mehr über technische Aspekte, was Ihnen beim Installieren und Konfigurieren der Identity Manager-Komponenten zugute kommt.

Nachdem Sie Ihre Entwicklungsumgebung eingerichtet haben, besteht der nächste Schritt darin, den Projektplan zum Implementieren der Identity Manager-Lösung zu erstellen. Verwenden Sie zum Erstellen des Projektplans die Informationen in Kapitel 2, „Erstellen eines Projektplans“, auf Seite 13.

2 Erstellen eines Projektplans

Das Planungsmaterial bietet einen Überblick über die Aktivitäten, die normalerweise Teil eines Identity Manager-Projekts sind - von den Anfängen bis zur vollständigen Produktionsbereitstellung. Zur Implementierung einer Identitätsmanagementstrategie müssen Sie Ihre aktuellen Geschäftsprozesse, die Erfordernisse dieser Prozesse sowie die Projektbeteiligten in der Umgebung kennen. Auf dieser Basis können Sie dann eine Lösung entwickeln, die Unterstützung der Projektbeteiligten einholen, die Lösung testen und ein Produktions-Rollout durchführen. In diesem Abschnitt werden die Grundlagen dieses Prozesses erläutert, damit Sie aus Identity Manager den bestmöglichen Nutzen ziehen können.

Dieser Abschnitt erhebt keinen Anspruch auf Vollständigkeit. Es werden weder alle möglichen Konfigurationen erläutert noch müssen die dargestellten Schritte zwingend ausgeführt werden. Jede Umgebung ist anders, sodass die Art der zu verwendenden Aktivitäten flexibel gehandhabt werden muss.

- Abschnitt 2.1, „Ermittlungsphase“, auf Seite 13
- Abschnitt 2.2, „Anforderungs- und Entwurfsanalysephase“, auf Seite 17
- Abschnitt 2.3, „Proof-of-Concept“, auf Seite 22
- Abschnitt 2.4, „Validierung und Vorbereitung der Daten“, auf Seite 22
- Abschnitt 2.5, „Produktions-Prototyp“, auf Seite 23
- Abschnitt 2.6, „Planung des Produktions-Rollout“, auf Seite 23
- Abschnitt 2.7, „Produktionsbereitstellung“, auf Seite 24

2.1 Ermittlungsphase

Die Identity Manager-Lösung wirkt sich auf viele Aspekte Ihres Unternehmens aus. Für eine effektive Lösung wird ausreichend Zeit benötigt, um alle aktuellen Geschäftsprozesse zu definieren, um herauszufinden, wie sich eine Implementierung der Identity Manager-Änderungen auf diese Prozesse auswirkt, auf welche Bereiche diese Änderungen Auswirkungen haben und wie die Änderungen implementiert werden.

In der Ermittlungsphase erhalten alle Projektbeteiligten einen allgemeinen Einblick in die Probleme und Lösungen. In dieser Phase wird eine Roadmap mit den wichtigsten Geschäfts- und Systeminformationen erstellt, die von der Identity Manager-Lösung betroffen sind. Zudem haben alle Projektbeteiligten die Möglichkeit, an der Erstellung der Identity Manager-Lösung mitzuwirken, damit sie wissen, wie sich diese auf ihr jeweiliges Geschäftsfeld auswirkt.

In der folgenden Liste werden die Schritte aufgeführt, die für eine erfolgreiche Ermittlungsphase erforderlich sind. Im Laufe der Ermittlungs- und Entwurfsphase werden Sie möglicherweise feststellen, dass Sie zusätzliche Schritte benötigen.

- Abschnitt 2.1.1, „Definieren aktueller Geschäftsprozesse“, auf Seite 14
- Abschnitt 2.1.2, „Definieren, wie sich die Identity Manager-Lösung auf die aktuellen Geschäftsprozesse auswirkt“, auf Seite 15
- Abschnitt 2.1.3, „Identifizieren der wichtigsten Projektbeteiligten auf geschäftlicher und technischer Ebene“, auf Seite 16
- Abschnitt 2.1.4, „Gespräche mit allen Projektbeteiligten führen“, auf Seite 16
- Abschnitt 2.1.5, „Erstellen einer allgemeinen Strategie und eines konsensfähigen Ausführungsablaufs“, auf Seite 17

2.1.1 Definieren aktueller Geschäftsprozesse

Identity Manager automatisiert Geschäftsprozesse, damit Identitäten in Ihrer Umgebung einfach verwaltet werden können. Wenn Sie die aktuellen Geschäftsprozesse nicht kennen, können Sie keine Identity Manager-Lösung entwerfen, die diese Prozesse automatisiert. Im Architektenmodus von Designer können Sie Ihre aktuellen Geschäftsprozesse erfassen und diese grafisch darstellen. Weitere Informationen finden Sie unter “Architect Mode” (Architektenmodus) im *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide* (Administrationshandbuch zu Designer 4.0.1 für Identity Manager 4.0.1).

Ihr Unternehmen könnte beispielsweise folgende Geschäftsprozesse identifizieren:

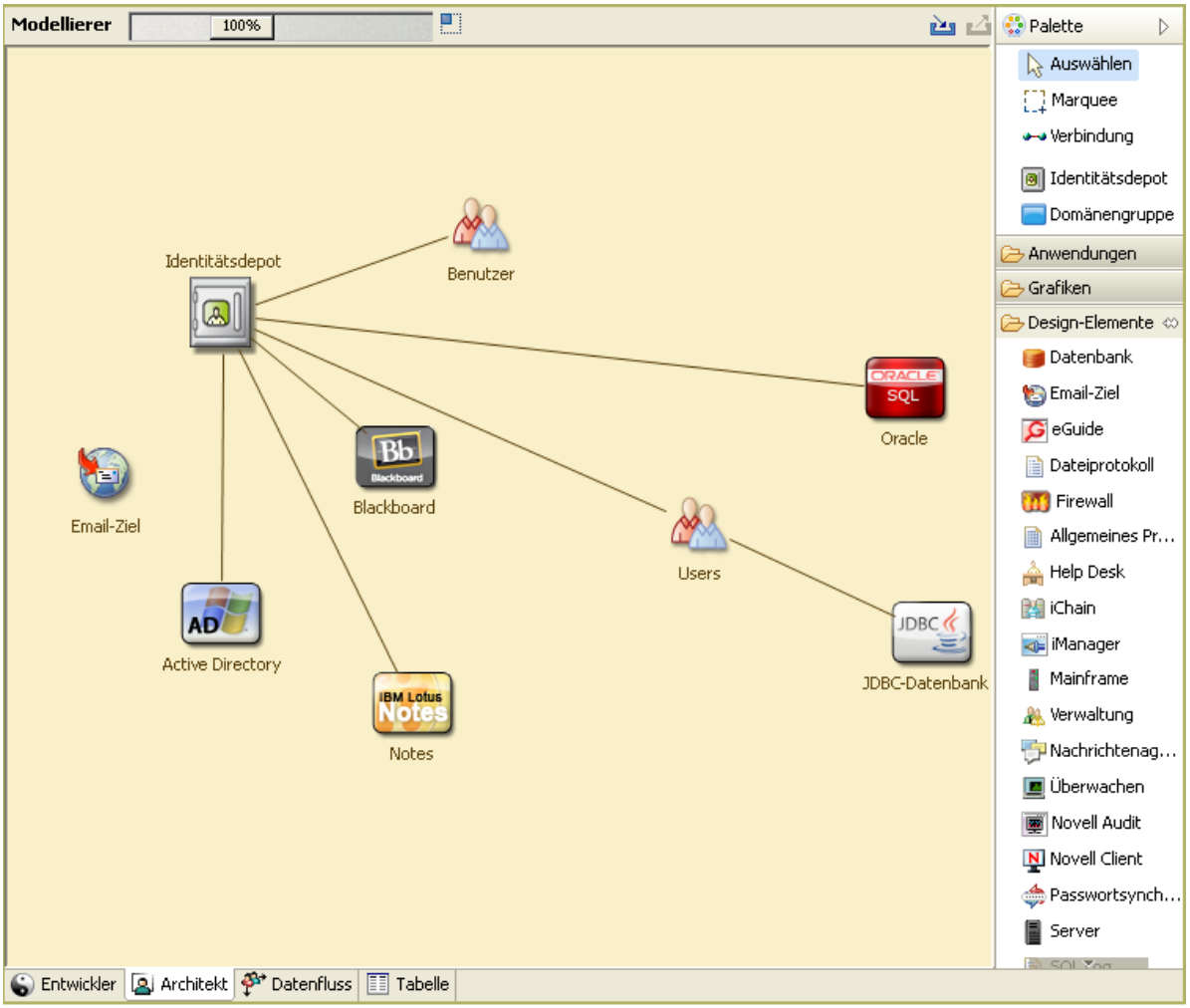
- Wenn ein Mitarbeiter ausscheidet, wird sein Benutzerkonto im Email-System gelöscht, aber das Benutzerkonto in allen anderen Systemen wird nicht gelöscht, sondern deaktiviert.
- Das Format einer Email-Adresse eines Benutzers.
- Die Systeme oder Ressourcen, auf die Vertriebsmitarbeiter zugreifen können.
- Die Systeme oder Ressourcen, auf die Manager zugreifen können.
- Welche Systeme erzeugen neue Konten? Das Personalsystem oder geschieht dies durch eine Workflow-Anforderung?
- Eine Passwortrichtlinie für das Unternehmen, anhand der definiert wird, wie oft ein Passwort geändert wird, wie komplex das Passwort ist und welche Systeme das Passwort synchronisieren.

Sie sollten beim Definieren von Geschäftsprozessen wie folgt vorgehen, um alle Prozesse zu verstehen:

- Definieren Sie die aktuellen Geschäftsaspekte.
- Legen Sie die Initiativen fest, die zum Angehen dieser Probleme erforderlich sind.
- Ermitteln Sie, welche Services und Systeme von diesen Initiativen betroffen sind.

Anhand dieser Schritte erhalten Sie einen allgemeinen Überblick über die aktuellen Abläufe bzw. Prozesse in Ihrem Unternehmen und können ermitteln, welche Prozesse verbessert werden müssen. Zum Beispiel verwendet Abbildung 2-1 Designer, um zu zeigen, wie neue Benutzerkonten vom PeopleSoft-System generiert werden. Sie werden in das Identitätsdepot und anschließend in Lotus Notes und Active Directory synchronisiert. Passwörter werden zwischen Active Directory und dem Identitätsdepot synchronisiert. Konten werden in das Notes-System synchronisiert, es werden aber keine Konten zurück in das Identitätsdepot synchronisiert.

Abbildung 2-1 *Beispiel für Geschäftsprozesse*



Nach dem Festlegen von Prozessen beginnen Sie zu untersuchen, wie Identity Manager eingesetzt werden kann. Fahren Sie mit Abschnitt 2.1.2, „Definieren, wie sich die Identity Manager-Lösung auf die aktuellen Geschäftsprozesse auswirkt“, auf Seite 15 fort.

2.1.2 Definieren, wie sich die Identity Manager-Lösung auf die aktuellen Geschäftsprozesse auswirkt

Nachdem Sie die aktuellen Geschäftsprozesse definiert haben, müssen Sie entscheiden, welche Prozesse in die Identity Manager-Lösung aufgenommen werden sollen.

Am besten betrachten Sie die gesamte Lösung und priorisieren dann die Prozesse, die implementiert werden sollen. Identity Manager umfasst so viele Aspekte Ihrer geschäftlichen Aktivitäten, dass es einfacher ist, eine Gesamtlösung zu planen, anstatt für jeden Geschäftsprozess eine eigene Lösung zu finden.

Erstellen Sie eine Liste der Geschäftsprozesse, die zuerst automatisiert werden sollen, und ermitteln Sie anschließend, auf welche Systeme sich diese Änderungen auswirken. Fahren Sie dann mit Abschnitt 2.1.3, „Identifizieren der wichtigsten Projektbeteiligten auf geschäftlicher und technischer Ebene“, auf Seite 16 fort.

2.1.3 Identifizieren der wichtigsten Projektbeteiligten auf geschäftlicher und technischer Ebene

Das Identifizieren aller Projektbeteiligten an der Identity Manager-Lösung ist für den Erfolg der Lösung enorm wichtig. In den meisten Firmen gibt es mehrere Kontaktpersonen, die alle geschäftlichen und technischen Aspekte der Geschäftsprozesse kennen. Sie müssen ermitteln, welche Services und Systeme von der Identity Manager-Lösung betroffen sind und wer für diesen Service oder dieses System verantwortlich ist.

Wenn Sie beispielsweise ein Email-System in Ihre Lösung integrieren, müssen Sie das Email-System, den Email-Systemadministrator ist und die verfügbaren Kontaktinformationen aufführen. Sie können all diese Informationen in das Designer-Projekt übernehmen. Jedes Anwendungssymbol bietet einen Ort, an dem Sie Informationen über das System und den Systemadministrator speichern können. Weitere Informationen finden Sie unter "Configuring Application Properties" (Eigenschaften dieser Anwendung konfigurieren) im *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide* (Administrationshandbuch zu Designer 4.0.1 für Identity Manager 4.0.1).

Nachdem Sie alle handelnden Personen eines jeden Geschäftsprozesses identifiziert haben, können Sie mit dem nächsten Schritt in Abschnitt 2.1.4, „Gespräche mit allen Projektbeteiligten führen“, auf Seite 16 fortfahren.

2.1.4 Gespräche mit allen Projektbeteiligten führen

Anhand von Gesprächen mit den wichtigsten Projektbeteiligten auf geschäftlicher und technischer Ebene können Sie Informationen sammeln, die Sie für einen vollständigen Entwurf einer Identity Manager-Lösung benötigen. Sie können die Gespräche auch dazu nutzen, die Projektbeteiligten über die Identity Manager-Lösung zu informieren und ihnen mitzuteilen, wie sich die Lösung auf ihre Bereiche auswirkt. Folgende Aspekte sollten bei Interviews abgedeckt werden:

- Definieren der Geschäftsprozesse, die von der Identity Manager-Lösung berührt werden. Der Gesprächspartner verfügt möglicherweise über Informationen, die eine Anpassung des aktuellen Plans erforderlich machen.
- Ermitteln, wie sich die Lösung auf die Projektbeteiligten auswirkt, und Eingehen auf mögliche Bedenken. Fragen Sie außerdem die Projektbeteiligten, wie viel Zeit ihr Beitrag zur Lösung in Anspruch nehmen wird. Die Interviewten können dies evtl. abschätzen und Sie können diese Informationen zur Ermittlung des Arbeitsaufwands für die Lösung heranziehen.
- Erfassen der wichtigsten Geschäfts- und Systeminformationen von den Projektbeteiligten. Manchmal kann sich ein Vorschlag nachteilig auf einen Geschäftsprozess oder ein System auswirken. Das Erfassen wichtiger Informationen hilft Ihnen, im Rahmen der Identity Manager-Lösung fundierte Entscheidungen zu treffen.

Nachdem Sie die wichtigsten Projektbeteiligten befragt haben, können Sie mit dem nächsten Schritt in Abschnitt 2.1.5, „Erstellen einer allgemeinen Strategie und eines konsensfähigen Ausführungsablaufs“, auf Seite 17 fortfahren.

2.1.5 Erstellen einer allgemeinen Strategie und eines konsensfähigen Ausführungsablaufs

Wenn alle Informationen zusammengestellt wurden, müssen Sie eine allgemeine Strategie bzw. eine Roadmap für die Identity Manager-Lösung entwerfen. Legen Sie alle Funktionen fest, die in der Identity Manager-Lösung berücksichtigt werden sollen. Neue Benutzerkonten werden beispielsweise durch eine Anforderung über einen Workflow generiert, aber der erstellte Benutzertyp hängt von den Ressourcen ab, auf die der Benutzer zugreifen kann.

Stellen Sie diese allgemeine Strategie, falls möglich, in einem einzigen Meeting allen Projektbeteiligten vor. Dies ermöglicht Ihnen mehrere Dinge:

- Sie können sich vergewissern, dass die beabsichtigten Initiativen berechtigt sind und welche die höchste Priorität haben.
- Identifizieren Sie die Planungsaktivitäten in Vorbereitung der Anforderungs- und Entwurfsphase.
- Legen Sie die Elemente fest, die zum Durchführen einer oder mehrerer dieser Initiativen erforderlich sind.
- Erstellen Sie einen konsensfähigen Ausführungspfad für die Identity Manager-Lösung.
- Definieren Sie zusätzliche Schulungen für die Projektbeteiligten.

Mit der Ermittlung erhalten alle Projektbeteiligten einen allgemeinen Einblick in die Probleme und Lösungen. Diese Phase bietet einen hervorragenden Ausgangspunkt für die Analysephase, für die die Projektbeteiligten Grundkenntnisse von Verzeichnissen sowie von Novell eDirectory, Novell Identity Manager und der XML-Integration im Allgemeinen benötigen.

Nachdem Sie die Ermittlungsphase abgeschlossen haben, fahren Sie mit Abschnitt 2.2, „Anforderungs- und Entwurfsanalysephase“, auf Seite 17 fort.

2.2 Anforderungs- und Entwurfsanalysephase

Verwenden Sie die in der Ermittlungsphase erstellte allgemeine Roadmap als Ausgangspunkt für die Analysephase. Sowohl das Dokument als auch das Designer-Projekt benötigen zusätzliche technische und geschäftliche Details. Daraus ergibt sich das Datenmodell und der allgemeine Entwurf der Identity Manager-Architektur, anhand der die Identity Manager-Lösung implementiert wird.

Der Entwurf sollte besonders das Identitätsmanagement umfassen. Es können aber auch viele Elemente, die traditionell einem Ressourcen-Management-Verzeichnis, z. B. Archivierung und Drucken, zugeordnet sind. Identity Manager synchronisiert Benutzerkonten mit Verzeichnissen, die keinen direkten Zugriff auf das Dateisystem des Betriebssystems haben. Beispielsweise können Sie ein Benutzerkonto in Active Directory haben, aber dies gewährt Ihnen keinen Zugriff auf das Dateisystem auf dem Active Directory-Server.

Beantworten Sie anhand der in der Ermittlungsphase gesammelten Informationen die folgenden Beispielfragen, um herauszufinden, ob Sie noch weitere Informationen benötigen. Möglicherweise müssen Sie dazu zusätzliche Interviews mit Projektbeteiligten führen.

- Welche Versionen der Systemsoftware werden verwendet?
- Ist der eDirectory-Entwurf zweckdienlich? Enthält der Identity Manager-Server beispielsweise eine Master- oder eine Lese-/Schreibreproduktion der Benutzerobjekte, die synchronisiert werden? Falls nicht, ist der eDirectory-Entwurf nicht zweckdienlich.

- Ist die Qualität der Daten in allen Systemen sachgemäß? (Wenn die Daten nicht verwendet werden können, wird die Geschäftsrichtlinie möglicherweise nicht wie gewünscht implementiert.) Es gibt beispielsweise doppelte Konten für die Benutzer in den Systemen, die synchronisiert werden, oder das Format der Daten ist innerhalb des Systems nicht konsistent. Die Daten eines jeden Systems müssen vor der Synchronisierung der Informationen evaluiert werden.
- Ist in Ihrer Umgebung eine Bearbeitung der Daten erforderlich? Beispielsweise ist das Format des Einstellungsdatums eines Benutzers im Personalsystem 23.02.2008 und im Identitätsdepot 23/02/2008. Dies bedeutet, dass das Datum zuerst bearbeitet werden muss, damit eine Synchronisierung erfolgen kann.

Identity Manager verfügt über ein Werkzeug, mit dem sich Daten einfacher analysieren und bereinigen lassen. Weitere Informationen hierzu finden Sie im *Analyzer 4.0.2 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.1 für Identity Manager).

Machen Sie sich mit den Informationen in Kapitel 3, „Technische Richtlinien“, auf Seite 25 vertraut, damit Sie für Ihre Umgebung die richtigen Entscheidungen treffen können.

Nach der Analyse der Anforderungen können Sie den Bereich und den Projektplan für die Implementierung erstellen und ermitteln, ob bestimmte Voraussetzungen erfüllt werden müssen. Sie sollten bei der Sammlung von Informationen und der Dokumentation der Anforderungen möglichst sorgfältig vorgehen, um kostspielige Fehler zu vermeiden. Hier ist eine Liste mit den möglichen Anforderungen:

- Datenmodell, das alle Systeme, autorisierte Datenursprünge, Ereignisse, Informationsfluss, Datenformatstandards sowie Zuordnungsbeziehungen zwischen verbundenen Systemen und Attributen in Identity Manager anzeigt.
- Geeignete Identity Manager-Architektur für die Lösung.
- Details für zusätzliche Systemverbindungsanforderungen.
- Strategien für die Datenvalidierung und das Auffinden übereinstimmender Datensätze.
- Entwurf der Verzeichnisse zur Unterstützung der Identity Manager-Infrastruktur.

Bei der Bewertung der Anforderungen und des Entwurfs sollten folgende Aufgaben durchgeführt werden:

- „Definieren der Geschäftsanforderungen“, auf Seite 18
- „Analysieren der Geschäftsprozesse“, auf Seite 20
- „Entwurf eines Enterprise-Datenmodells“, auf Seite 20

2.2.1 Definieren der Geschäftsanforderungen

In der Ermittlungsphase haben Sie Informationen zu den Geschäftsprozessen und -anforderungen Ihres Unternehmens gesammelt, die diese Geschäftsprozesse definieren. Erstellen Sie eine Liste dieser Geschäftsanforderungen und ordnen Sie anschließend in Designer diese Prozesse zu, indem Sie folgende Aufgaben durchführen:

- Erstellen Sie eine Liste der Geschäftsanforderungen und ermitteln Sie, welche Systeme von diesem Prozess beeinflusst werden. Beispiel: Eine Geschäftsanforderung bei der Kündigung eines Mitarbeiters könnte sein, dass am Tag der Kündigung der Zugriff des Mitarbeiters auf das Netzwerk und sein Email-Konto gesperrt wird. Dieser Kündigungsprozess wirkt sich auf das Email-System und das Identitätsdepot aus.
- Erstellen Sie Prozessabfolgen, Prozessauslöser und Datenzuordnungsbeziehungen.

Wenn beispielsweise etwas in einem bestimmten Prozess geschieht, welche anderen Prozesse werden dadurch ausgelöst?

- Ordnen Sie Datenflüsse zwischen Anwendungen zu. Diese Informationen werden in Designer angezeigt. Weitere Informationen finden Sie unter "Managing the Flow of Data" (Verwalten des Datenflusses) im *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide* (Administrationshandbuch zu Designer 4.0.1 für Identity Manager 4.0.1).
- Ermitteln Sie Daten, die von einem Format in ein anderes umgewandelt werden müssen, z. B. 2/25/2007 in 25. Februar 2007, und verwenden Sie Analyzer zum Ändern der Daten. Weitere Informationen hierzu finden Sie im *Analyzer 4.0.2 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.1 für Identity Manager).
- Dokumentieren Sie bestehende Datenabhängigkeiten.

  Wenn ein bestimmter Wert geändert wird, ist es wichtig zu wissen, ob für diesen Wert eine Abhängigkeit besteht. Wenn ein bestimmter Prozess geändert wird, ist es wichtig zu wissen, ob für diesen Prozess eine Abhängigkeit besteht.

  Wenn Sie z. B. in einem Human-Resources-System für einen Mitarbeiter den Status „Temporär" auswählen, hat dies möglicherweise zur Folge, dass die IT-Abteilung in eDirectory ein Benutzerobjekt mit eingeschränkten Rechten und einem auf bestimmte Zeiten begrenzten Netzwerkzugang erstellen muss.
- Listen Sie die Prioritäten auf.

  Es können nicht direkt die Anforderungen und Wünsche aller Personen erfüllt werden. Prioritäten für den Entwurf und die Bereitstellung des Bereitstellungssystems vereinfachen die Planung einer Roadmap.

  Es kann für Sie von Vorteil sein, die Bereitstellung in Phasen aufzuteilen, um einen Teil der Bereitstellung früher, andere Teile wiederum später zu implementieren. Sie können auch eine in Phasen aufgeteilte Bereitstellung durchführen, die auf Gruppen von Personen in der Organisation basiert.
- Definieren Sie die Voraussetzungen.

  Die für die Implementierung einer bestimmten Phase der Bereitstellung erforderlichen Voraussetzungen sollten dokumentiert werden. Dies umfasst den Zugriff auf die verbundenen Systeme, die mit Identity Manager gekoppelt werden sollen.
- Identifizieren Sie autorisierte Datenursprünge.

  Wenn Sie bereits früh wissen, welche Elemente welchen IT-Administratoren und -Managern zuzuordnen sind, kann dies bei allen beteiligten Parteien zu einer größeren Akzeptanz führen.

  Beispiel: Der Kontoadministrator benötigt möglicherweise die Berechtigung, Mitarbeitern Rechte für bestimmte Dateien und Verzeichnisse zu gewähren. Dieser Erfordernis kann Rechnung getragen werden, indem lokale Trustee-Zuweisungen in das Kontosystem implementiert werden.

Nachdem Sie die Geschäftsanforderungen definiert haben, fahren Sie mit Abschnitt 2.2.2, „Analysieren der Geschäftsprozesse", auf Seite 20 fort.

2.2.2 Analysieren der Geschäftsprozesse

Nachdem Sie die Analyse der Geschäftsanforderungen abgeschlossen haben, benötigen Sie für die genaue Abstimmung der Identity Manager-Lösung noch weitere Informationen. Sie müssen wichtige Personen wie Manager, Administratoren und Mitarbeiter interviewen, die die Anwendung oder das System einsetzen. Folgende Fragen sollten beantwortet werden:

- Woher stammen die Daten?
- Wofür sind die Daten bestimmt?
- Wer ist für die Daten verantwortlich?
- Wer ist der Eigentümer der Geschäftsfunktion, zu der die Daten gehören?
- Wer muss zur Änderung der Daten kontaktiert werden?
- Welche Folgen hat die Änderung von Daten?
- Welche Arbeitsmethoden gelten für die Datenbearbeitung (Sammeln und/oder Bearbeitung)?
- Welche Art von Vorgängen laufen ab?
- Welche Methoden werden zur Sicherung der Datenqualität und -integrität verwendet?
- Wo werden die Systeme eingesetzt (auf welchen Servern, in welchen Abteilungen)?
- Welche Prozesse eignen sich nicht für die automatisierte Bearbeitung?

Sie können beispielsweise einem Administrator eines PeopleSoft-Systems in der Personalabteilung folgende Fragen stellen:

- Welche Daten werden in der PeopleSoft-Datenbank gespeichert?
- Welche Elemente werden in den verschiedenen Teilfenstern eines Mitarbeiterkontos angezeigt?
- Welche Aktionen müssen über das gesamte Bereitstellungssystem hinweg durchgeführt werden (z. B. Aktionen zum Hinzufügen, Modifizieren und Löschen)?
- Welche dieser Aktionen sind erforderlich? Welche Aktionen sind optional?
- Welche Aktionen müssen auf Basis der in PeopleSoft durchgeführten Aktionen ausgelöst werden?
- Welche Operationen/Ereignisse/Aktionen müssen ignoriert werden?
- Auf welche Weise müssen die Daten transformiert und Identity Manager zugeordnet werden?

Das Befragen wichtiger Personen kann Sie in andere Bereiche der Organisation führen, durch die Sie ein deutlicheres Bild des gesamten Prozesses gewinnen können.

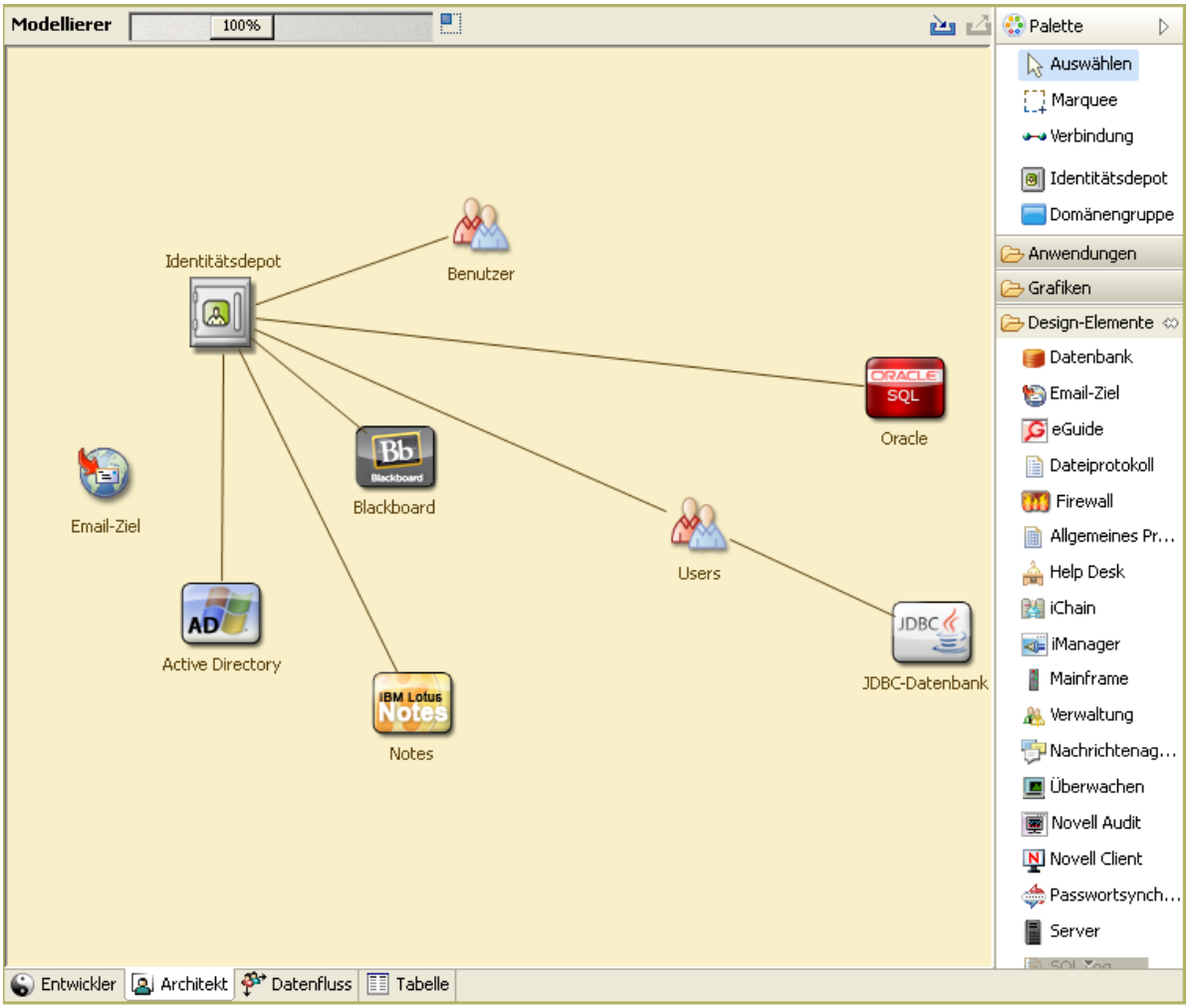
Wenn Sie all diese Informationen gesammelt haben, können Sie ein Enterprise-Datenmodell für Ihre Umgebung entwerfen. Fahren Sie mit Abschnitt 2.2.3, „Entwurf eines Enterprise-Datenmodells“, auf Seite 20 fort, um mit dem Entwurf zu beginnen.

2.2.3 Entwurf eines Enterprise-Datenmodells

Nach der Definition der Geschäftsprozesse können Sie unter Verwendung von Designer mit dem Entwurf eines Datenmodells beginnen, das Ihre aktuellen Geschäftsprozesse widerspiegelt.

Das Modell in Designer gibt den Datenursprung sowie die Richtung des Datenflusses an und zeigt auf, wohin sich die Daten nicht bewegen dürfen. Außerdem wird aufgezeigt, auf welche Weise sich kritische Ereignisse auf den Datenfluss auswirken. Zum Beispiel zeigt Abbildung 2-2 den Datenfluss zwischen dem Identitätsdepot und verschiedenen verbundenen Systemen.

Abbildung 2-2 *Datenfluss in Designer*



Möglicherweise empfiehlt sich auch die Entwicklung eines Diagramms, das den vorgeschlagenen Geschäftsprozess und die Vorteile veranschaulicht, die durch die Implementierung der automatisierten Bereitstellung erzielt werden.

Am Anfang der Entwicklung dieses Modells steht die Beantwortung folgender Fragen:

- Welche Objekttypen (z. B. Benutzer oder Gruppen) werden verschoben?
- Welche Ereignisse sind von Interesse?
- Welche Attribute müssen synchronisiert werden?
- Welche Daten werden in Ihrem Unternehmen für die verschiedenen zu verwaltenden Objekttypen gespeichert?
- Handelt es sich um eine einseitige oder um eine bidirektionale Synchronisierung?
- Welches System ist für welche Attribute der autorisierte Ursprung?

Außerdem ist es wichtig, die Zusammenhänge verschiedener Werte zwischen den Systemen zu berücksichtigen.

Das Statusfeld eines Mitarbeiters in PeopleSoft kann beispielsweise drei Werte annehmen: „Festangestellter“, „Freiberufler“ und „Praktikant“. Das Active Directory-System hat möglicherweise nur zwei Werte: „Dauerhaft“ und „Temporär“. In diesem Fall müssen die Beziehungen zwischen dem Status „Freiberufler“ in PeopleSoft und den Werten „Dauerhaft“ und „Temporär“ in Active Directory festgelegt werden.

Ziel dieser Tätigkeit ist es, alle Verzeichnissysteme zu verstehen, in welcher Beziehung sie zueinander stehen und welche Objekte und Attribute systemübergreifend synchronisiert werden müssen. Nach der Fertigstellung des Entwurfs besteht der nächste Schritt darin, ein Proof-of-Concept zu erstellen. Fahren Sie mit Abschnitt 2.3, „Proof-of-Concept“, auf Seite 22 fort.

2.3 Proof-of-Concept

Sie erstellen und testen ein Proof-of-Concept, indem Sie eine Beispielimplementierung in einer Testumgebung durchführen, bei der Sie die Geschäftsrichtlinien und den Datenfluss Ihres Unternehmens simulieren. Die Implementierung basiert auf dem Datenmodell, das während der Anforderungsanalyse und der Entwurfsphase entwickelt wurde. Dies ist der letzte Schritt vor dem Produktions-Prototyp. Sie führen die Tests in der Testumgebung durch, die Sie unter Kapitel 1, „Einrichten einer Entwicklungsumgebung“, auf Seite 11 erstellt haben.

Hinweis: In dieser Phase bietet es sich an, die Unterstützung des Managements einzuholen und die Finanzierung für die endgültige Umsetzung zu sichern.

Kapitel 3, „Technische Richtlinien“, auf Seite 25 enthält Informationen, die für die Validierung des Proof-of-Concept nützlich sind. Es enthält technische Richtlinien, die Sie bei einer erfolgreichen Identity Manager-Bereitstellung unterstützen.

Neben der Erstellung des Proof-of-Concept müssen Sie auch einen Plan zur Validierung der Daten erstellen, die sich in Ihren Systemen befinden. Mithilfe dieses Schritts stellen Sie sicher, dass keine Konflikte zwischen den Systemen auftreten. Fahren Sie mit Abschnitt 2.4, „Validierung und Vorbereitung der Daten“, auf Seite 22 fort. Dort finden Sie Informationen darüber, wie Sie diese Konflikte verhindern können.

2.4 Validierung und Vorbereitung der Daten

Die Qualität und Konsistenz der Daten in Produktionssystemen kann variieren und möglicherweise Inkonsistenzen bei der Synchronisierung von Systemen zur Folge haben. In dieser Phase wird eine deutliche Trennung zwischen dem Team, das für die Implementierung der Ressourcen zuständig ist,

und den Geschäftseinheiten oder -gruppen vorgenommen, die „Eigentümer“ der Daten in den zu integrierenden Systemen sind oder diese verwalten. Bestehende Risiko- und Kostenfaktoren gehören nicht unbedingt zu einem Bereitstellungsprojekt.

Sie benötigen das Datenmodell, das Sie in den Analyse- und Entwurfsphasen entwickelt haben. Sie sollten auch über eine mögliche Strategie zum Datenformat und Datensatzabgleich verfügen, damit die Daten ordnungsgemäß vorbereitet werden können. Nachdem Sie die Datenmodell- und -formatstrategie definiert haben, können Sie zwei wichtige Schritte durchführen:

- Erstellen Sie Produktions-Daten-Sets, die in das Identitätsdepot geladen werden können (wie in den Analyse- und Entwurfsaktivitäten definiert). Hierzu gehört auch die Angabe der voraussichtlichen Lademethode (Bulk-Verarbeitung oder über Anschlüsse). Es werden auch Anforderungen für die Daten identifiziert, die validiert oder in bestimmter Weise formatiert werden.
- Identifizieren Sie Leistungsfaktoren und validieren Sie diese Faktoren auf der Grundlage der verwendeten Geräte und der allgemeinen verteilten Architektur der Identity Manager-Bereitstellung.

Fahren Sie nach der Vorbereitung der Daten mit Abschnitt 2.5, „Produktions-Prototyp“, auf Seite 23 fort.

2.5 Produktions-Prototyp

Der Produktions-Prototyp ist der erste Schritt bei der Migration in eine Produktionsumgebung. Während dieser Phase ist möglicherweise eine zusätzliche Anpassung erforderlich. In dieser kurzen Einführung können die gewünschten Ergebnisse der vorhergehenden Aktivitäten bestätigt und die Zustimmung für das Produktions-Rollout eingeholt werden. Anhand der Prototyp-Lösung wird der Plan validiert, der bis zu diesem Zeitpunkt im Prozess erstellt wurde.

Hinweis: Diese Phase liefert möglicherweise die Abnahmekriterien für die Lösung und den benötigten Meilenstein auf dem Weg zur vollständigen Produktion.

Die Prototyp-Lösung bietet ein Live-Proof-of-Concept und eine Validierung des Datenmodells sowie der gewünschten Prozessergebnisse. Fahren Sie nach Fertigstellung des Prototyps mit Abschnitt 2.6, „Planung des Produktions-Rollout“, auf Seite 23 fort.

2.6 Planung des Produktions-Rollout

In dieser Phase wird die Produktionsumgebung geplant. Der Plan sollte mehrere Dinge umfassen:

- Bestätigung der Serverplattformen, Softwareversionen und Service Packs
- Bestätigung der allgemeinen Umgebung
- Bestätigung des Entwurfs des Identitätsdepots in einer gemischten Umgebung
- Bestätigung, dass die Geschäftslogik korrekt ist
- Bestätigung, dass die Datensynchronisierung wie geplant ausgeführt wird
- Planung der Umstellung auf den neuen Prozess
- Planung einer Rollback-Strategie für den Notfall

Der Plan muss Datumsangaben für die Implementierung und Fertigstellung der einzelnen Schritte des Rollouts enthalten. Jeder Projektbeteiligte liefert Input zu diesen Datumsangaben und stimmt den festgelegten Terminen zu. Dadurch wissen alle am Rollout beteiligten Personen, wann die Änderungen zu erwarten und wann sie abgeschlossen sind.

Wenn der Plan für das Produktions-Rollout fertig ist, fahren Sie mit Abschnitt 2.7, „Produktionsbereitstellung“, auf Seite 24 fort.

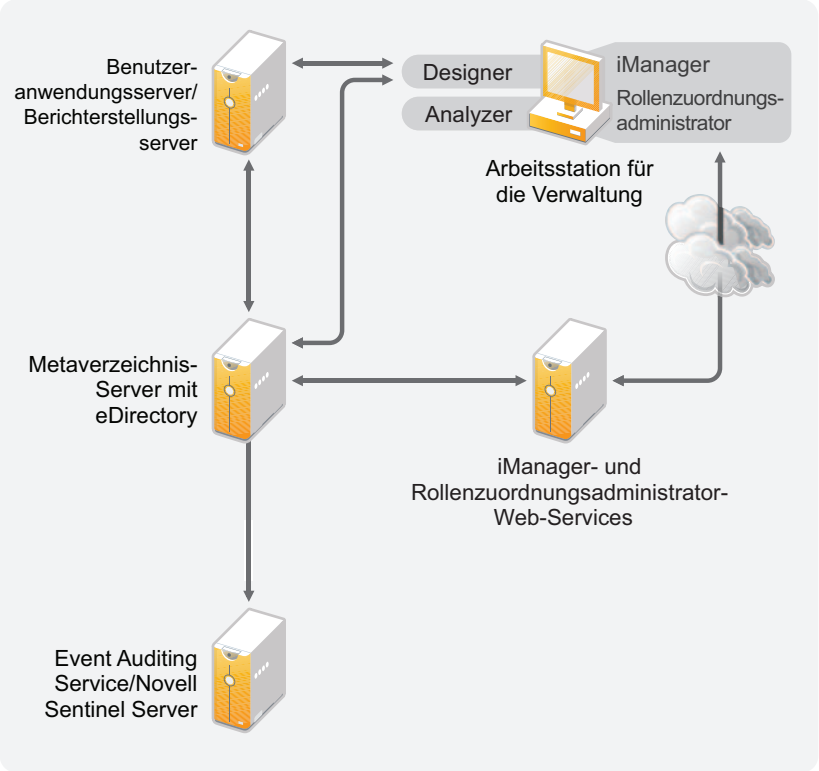
2.7 Produktionsbereitstellung

In der Produktionsbereitstellungsphase werden alle Pläne umgesetzt und die Identity Manager-Lösung wird in der Live-Umgebung implementiert. Mit dem Plan für das Produktions-Rollout können Sie die verschiedenen Teile der Identity Manager-Lösung in Betrieb nehmen. Je nachdem, wie komplex der Plan ist, kann dies schnell gehen oder einige Zeit dauern.

3 Technische Richtlinien

Auf Basis der in Designer gesammelten Informationen können Sie zu jeder Komponente von Identity Manager technische Entscheidungen treffen, z. B. über den Installationsspeicherort und Konfigurationsoptionen. Eine Einführung zu jeder Komponente finden Sie im *Identity Manager 4.0.2 Übersichtshandbuch*. Abbildung 3-1 ist eine mögliche Konfiguration einer Identity Manager-Lösung.

Abbildung 3-1 *Identity Manager-Komponenten*



Identity Manager kann sehr variabel auf die eigenen Erfordernisse angepasst werden. Folgende Abschnitte enthalten technische Richtlinien zu den Best Practices, wodurch die am besten für Ihre Umgebung geeignete Identity Manager-Lösung einfacher eingerichtet und konfiguriert werden kann. Zu den Variablen, die beeinflussen, wie diese Richtlinien auf Ihre Umgebung angewendet werden können, gehören der Hardwaretyp Ihrer Server, wie Ihr WAN konfiguriert ist und wie viele Objekte synchronisiert werden.

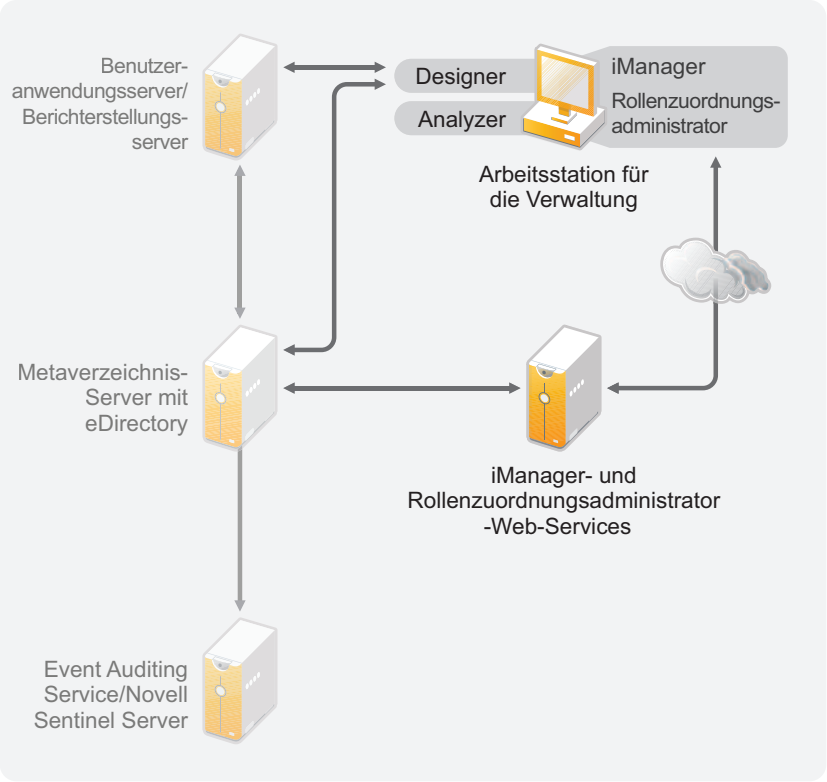
- Abschnitt 3.1, „Verwaltungswerkzeuge - Richtlinien“, auf Seite 26
- Abschnitt 3.2, „Metaverzeichnis-Server-Richtlinien“, auf Seite 28
- Abschnitt 3.3, „eDirectory-Richtlinien“, auf Seite 29

- Abschnitt 3.4, „Benutzeranwendung“, auf Seite 34
- Abschnitt 3.5, „Revision und Berichterstellung - Richtlinien“, auf Seite 34

3.1 Verwaltungswerkzeuge - Richtlinien

Die beiden Verwaltungswerkzeuge für die Identity Manager-Lösung sind Designer und iManager, wie in Abbildung 3-2 dargestellt. Designer wird für die Planung und Erstellung und iManager für die täglichen Verwaltungsaufgaben der Identity Manager-Lösung verwendet.

Abbildung 3-2 *Identity Manager - Verwaltungswerkzeuge*



Die Benutzeranwendung verwendet eine webbasierte Verwaltungsseite. Weitere Informationen über die Benutzeranwendung finden Sie unter “Administering the User Application” (Benutzeranwendung verwalten) im *User Application: Administration Guide* (Rollenbasiertes Bereitstellungsmodul für Identity Manager 4.0 Benutzeranwendung: Administrationshandbuch).

- Abschnitt 3.1.1, „Analyzer-Richtlinien“, auf Seite 27
- Abschnitt 3.1.2, „Designer-Richtlinien“, auf Seite 27
- Abschnitt 3.1.3, „iManager-Richtlinien“, auf Seite 27
- Abschnitt 3.1.4, „Rollenzuordnungsadministrator-Richtlinien“, auf Seite 27

3.1.1 Analyzer-Richtlinien

Analyzer ist ein Thick-Client, der auf einer Arbeitsstation installiert wird. Analyzer wird zum Untersuchen und Bereinigen der Daten in den Systemen verwendet, die Sie in Ihre Identity Manager-Lösung einbinden möchten. Wenn Sie Analyzer in der Planungsphase verwenden, können Sie sehen, welche Änderungen vorgenommen werden müssen und was hierfür die beste Methode ist.

Es sind keine wichtigen Faktoren bei der Verwendung von Analyzer zu beachten. Weitere Informationen hierzu finden Sie im *Analyzer 4.0.2 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.1 für Identity Manager).

3.1.2 Designer-Richtlinien

Designer ist ein Thick-Client, der auf einer Arbeitsstation installiert wird. Designer wird zum Entwerfen, Testen, Dokumentieren und Bereitstellen Ihrer Identity Manager-Lösung verwendet. Die Verwendung von Designer über die gesamte Planungsphase hinweg hilft Ihnen bei der zentralen Erfassung von Informationen. Sie erhalten zudem einen Überblick über alle Komponenten der Lösung, wodurch Sie Probleme besser erkennen können.

Bei der Verwendung von Designer gibt es keine weiteren Aspekte zu beachten, sofern nicht mehrere Personen an demselben Projekt arbeiten. Designer ermöglicht die Versionskontrolle des Projekts. Weitere Informationen finden Sie unter "Version Control" (Versionskontrolle) im *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide* (Administrationshandbuch zu Designer 4.0.1 für Identity Manager 4.0.1).

3.1.3 iManager-Richtlinien

iManager ist eine Webanwendung, die als Verwaltungswerkzeug für Identity Manager dient. Wenn Sie Identity Manager installieren, wird bei der Installation vorausgesetzt, dass Sie bereits einen iManager-Server in Ihrem eDirectory-Baum installiert haben.

Wenn mehr als zehn Administratoren dauerhaft gleichzeitig in iManager arbeiten, sollten Sie über einen Server verfügen, der ausschließlich iManager hostet. Abbildung 3-2 stellt diese Konfiguration Ihrer Identity Manager-Lösung dar. Gibt es nur einen Administrator, können Sie iManager ohne Probleme auf Ihrem Metaverzeichnis-Server ausführen.

3.1.4 Rollenzuordnungsadministrator-Richtlinien

Der Rollenzuordnungsadministrator ist eine Webanwendung, die die Autorisierungen und Berechtigungen ermittelt, die innerhalb Ihres Haupt-IT-Systems erteilt werden können. Er ermöglicht es Geschäftsanalysten, nicht nur IT-Administratoren, bestimmte Autorisierungen für bestimmte Geschäftsrollen zu definieren und zu verwalten.

Bei der Verwendung des Rollenzuordnungsadministrators sind keine wichtigen Faktoren zu berücksichtigen. Sie können den Rollenzuordnungsadministrator auf einem separaten Server ausführen, wie in Abbildung 3-2 dargestellt, oder Sie können ihn auf dem Metaverzeichnis-Server ausführen. Weitere Informationen finden Sie im *Identity Manager Role Mapping Administrator 4.0.2 Installation and Configuration Guide* (Installations- und Konfigurationshandbuch zum Identity Manager-Rollenzuordnungsadministrator 4.0).

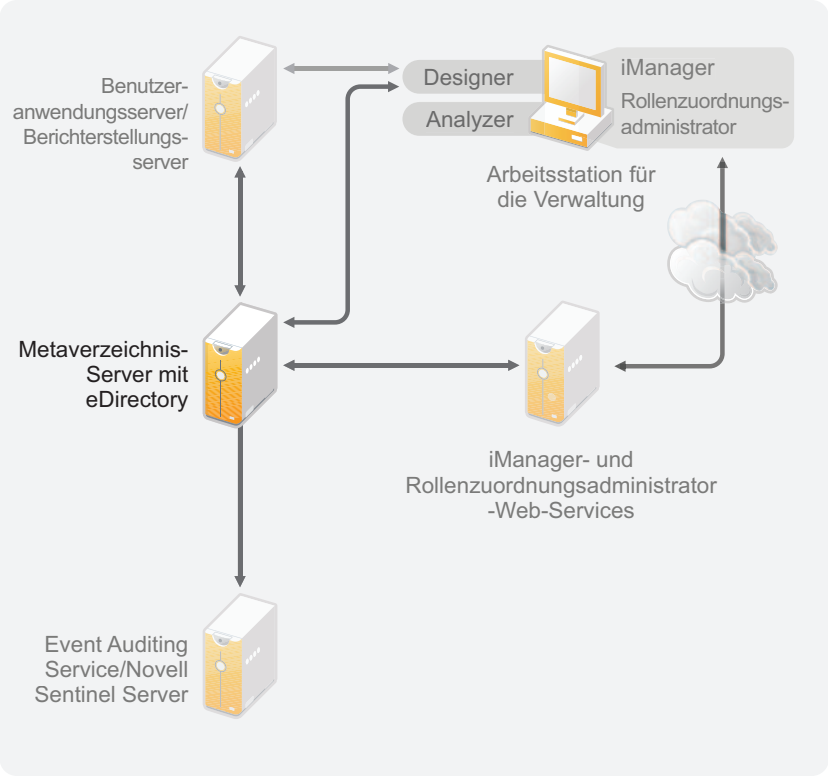
3.2 Metaverzeichnis-Server-Richtlinien

Abhängig von der Arbeitslast des Servers können Sie einen oder mehrere Metaverzeichnis-Server einsetzen. Für den Metaverzeichnis-Server ist es erforderlich, dass eDirectory installiert ist, wie in Abbildung 3-3 dargestellt. Sie können einen Remote Loader-Server hinzufügen (in der Abbildung nicht dargestellt), damit die Arbeitslast bzw. die Konfiguration Ihrer Umgebung besser bewältigt werden kann.

Die Treiber müssen auf demselben Server wie die verbundene Anwendung ausgeführt werden. Achten Sie beispielsweise beim Konfigurieren des Active Directory-Treibers darauf, dass der Server in Abbildung 3-3 ein Mitgliedsserver oder ein Domänencontroller sein muss. Wenn Sie eDirectory und Identity Manager nicht auf einem Mitgliedsserver oder Domänencontroller installieren möchten, können Sie den Remote Loader dort installieren. Der Remote Loader sendet alle Ereignisse von Active Directory an den Metaverzeichnis-Server. Der Remote Loader empfängt Informationen vom Metaverzeichnis-Server und übergibt sie an die verbundene Anwendung.

Der Remote Loader bietet zusätzliche Flexibilität für Ihre Identity Manager-Lösung. Weitere Informationen finden Sie im *Identity Manager 4.0.2 Remote Loader Guide* (Handbuch zu Identity Manager 4.0.1 Remote Loader).

Abbildung 3-3 *Metaverzeichnis-Server*



Es gibt viele Variablen, die sich auf die Arbeitsgeschwindigkeit des Servers auswirken. Allgemein wird empfohlen, nicht mehr als zehn Treiber auf einem Metaverzeichnis-Server auszuführen. Wenn allerdings jeder Treiber Millionen von Objekten synchronisiert, ist es u. U. nicht möglich, zehn Treiber auf einem Server auszuführen. Wenn Sie andererseits jedoch nur 100 Objekte pro Treiber synchronisieren, können Sie wahrscheinlich mehr als zehn Treiber auf einem Server ausführen.

Die Einrichtung der Identity Manager-Lösung in einer Testumgebung ermöglicht Ihnen, die Leistungsfähigkeit der Server zu testen. Die Zustandsüberwachungswerkzeuge in iManager liefern Ihnen Basisdaten, anhand derer Sie fundierte Entscheidungen für Ihre Umgebung treffen können. Weitere Informationen über die Werkzeuge zur Überwachung des Treiberzustands finden Sie unter "Monitoring Driver Health" (Überwachen des Treiberzustands) im *Identity Manager 4.0.2 Common Driver Administration Guide* (Administrationshandbuch zu Identity Manager 4.0.1 Common Driver).

Zu berücksichtigende Aspekte für die einzelnen Treiber finden Sie auf der Website zur Identity Manager Treiber-Dokumentation (http://www.novell.com/documentation/idm36drivers/index.html). In jedem Treiberhandbuch finden Sie die für den jeweiligen Treiber spezifischen Informationen.

3.3 eDirectory-Richtlinien

eDirectory ist das Identitätsdepot, in dem die Objekte gespeichert werden, die anhand der Identity Manager-Lösung synchronisiert werden. Die folgenden Abschnitte behandeln die Richtlinien, mit deren Hilfe Sie die Bereitstellung von eDirectory planen können.

- Abschnitt 3.3.1, „Identity Manager-Objekte in eDirectory“, auf Seite 29
- Abschnitt 3.3.2, „Reproduktion der von Identity Manager auf dem Server benötigten Objekte“, auf Seite 30
- Abschnitt 3.3.3, „Verwendung der Bereichsfilterung zum Verwalten von Benutzern auf verschiedenen Servern“, auf Seite 31

3.3.1 Identity Manager-Objekte in eDirectory

Die folgende Liste enthält die wesentlichen Identity Manager-Objekte, die in eDirectory gespeichert sind, und deren Verhalten zueinander . Während der Installation von Identity Manager werden keine Objekte erstellt. Die Identity Manager-Objekte werden im Rahmen der Konfiguration der Identity Manager-Lösung erstellt.

- **Treibersatz:** Ein Treibersatz ist ein Container, der Identity Manager-Treiber und Bibliotheksobjekte enthält. Auf einem Server kann immer nur ein Treibersatz aktiv sein. Sie können einen Treibersatz jedoch mit mehreren Servern verknüpfen. Ein Treiber kann auch mehreren Servern gleichzeitig zugeordnet werden. Er sollte jedoch immer nur auf einem Server gleichzeitig ausgeführt werden. Auf den anderen Servern muss der Treiber deaktiviert sein. Auf jedem mit einem Treibersatz verknüpften Server muss der Metaverzeichnis-Server installiert sein.
- **Bibliothek:** Das Bibliotheksobjekt ist ein Repository mit häufig verwendeten Richtlinien, das von mehreren Positionen aus referenziert werden kann. Die Bibliothek wird im Treibersatz gespeichert. Sie können eine Richtlinie in die Bibliothek stellen, damit jeder Treiber im Treibersatz auf sie verwiesen werden kann.
- **Treiber:** Ein Treiber stellt die Verbindung zwischen einer Anwendung und dem Identitätsdepot her. Er ermöglicht darüber hinaus die Datensynchronisierung und Datenfreigabe zwischen Systemen. Der Treiber wird im Treibersatz abgelegt.
- **Auftrag:** Ein Auftrag automatisiert eine wiederkehrende Aufgabe. Ein Auftrag kann beispielsweise ein System konfigurieren, um ein Konto an einem bestimmten Tag zu deaktivieren oder um einen Workflow zu starten, mit dem eine Erweiterung der Zugriffsrechte einer Person auf eine Unternehmensressource angefordert wird. Der Auftrag wird im Treibersatz abgelegt.

3.3.2 Reproduktion der von Identity Manager auf dem Server benötigten Objekte

Wenn in Ihrer Identity Manager-Umgebung mehrere Server benötigt werden, damit mehrere Identity Manager-Treiber ausgeführt werden können, sollten Sie dies in Ihrem Plan berücksichtigen und sicherstellen, dass bestimmte eDirectory-Objekte auf Servern reproduziert werden, auf denen die Identity Manager-Treiber ausgeführt werden sollen.

Sie können gefilterte Reproduktionen verwenden, sofern alle Objekte und Attribute, die der Treiber lesen oder synchronisieren muss, Teil der gefilterten Reproduktion sind.

Denken Sie daran, dem Identity Manager-Treiberobjekt ausreichende eDirectory-Rechte für die zu synchronisierenden Objekte zu erteilen. Gewähren Sie diese Rechte entweder explizit oder definieren Sie das Treiberobjekt als sicherheitsäquivalent mit einem Objekt, das über die gewünschten Rechte verfügt.

Ein eDirectory-Server, auf dem ein Identity Manager-Treiber ausgeführt wird (oder auf den der Treiber verweist, falls Sie den Remote Loader verwenden), muss eine Masterreproduktion oder eine Lese-/Schreibreproduktion der folgenden Elemente enthalten:

- Das Treibersatzobjekt für den Server.

  Für jeden Server, auf dem Identity Manager läuft, muss ein Treibersatzobjekt vorhanden sein. Sofern Sie keine speziellen Anforderungen haben, ordnen Sie nicht mehrere Server demselben Treibersatzobjekt zu.

  Hinweis: Beim Erstellen eines Treibersatzobjekts wird standardmäßig eine separate Partition erstellt. Es wird empfohlen, für das Treibersatzobjekt eine separate Partition zu erstellen. Damit Identity Manager funktioniert, muss der Server eine vollständige Reproduktion des Treibersatzobjekts enthalten. Wenn dem Server eine vollständige Reproduktion des Speicherorts zur Verfügung steht, an dem das Treibersatzobjekt installiert ist, wird keine Partition benötigt.

- Das Serverobjekt für den Treiber.

  Das Serverobjekt wird benötigt, damit der Treiber Schlüsselpaare für Objekte erstellen kann. Außerdem ist es wichtig für die Authentifizierung des Remote Loaders.

- Die Objekte, die diese Instanz des Treibers synchronisieren soll.

  Der Treiber kann nur Objekte synchronisieren, sofern sich eine Reproduktion dieser Objekte auf demselben Server befindet wie der Treiber. Der Identity Manager-Treiber synchronisiert die Objekte in *allen* Containern, die auf dem betreffenden Server repliziert sind, sofern Sie keine anderen Regeln für die Bereichsfilterung festgelegt haben.

  Wenn ein Treiber beispielsweise alle Benutzerobjekte synchronisieren soll, geschieht dies am einfachsten durch die Instanz eines Treibers auf dem Server, auf dem sich eine Lese-/Schreibreproduktion aller Benutzer befindet.

  In vielen Umgebungen gibt es jedoch keinen Einzelserver, der eine Reproduktion aller Benutzer enthält. Stattdessen sind die Benutzer-Datensätze auf mehrere Server verteilt. In diesem Fall stehen Ihnen drei Möglichkeiten zur Auswahl:

  - **Kumulierung aller Benutzer auf einem Server** Sie können einen Server erstellen, der alle Benutzer enthält, indem Sie zu einem vorhandenen Server Reproduktionen hinzufügen. Sofern erforderlich können gefilterte Reproduktionen verwendet werden, was die Größe der eDirectory-Datenbank verringert. Die erforderlichen Benutzerobjekte und -attribute müssen jedoch Teil der gefilterten Reproduktion sein.

- **Verwendung mehrerer Instanzen des Treibers auf mehreren Servern mit Bereichsfilterung.** Wenn Sie die Benutzer nicht auf einem Server kumulieren möchten, müssen Sie festlegen, welche Server alle Benutzer enthalten, und anschließend auf jedem dieser Treiber eine Instanz des Identity Manager-Treibers einrichten.

  Damit keine separaten Instanzen eines Treibers versuchen, dieselben Benutzer zu synchronisieren, müssen Sie in der Bereichsfilterung definieren, welche Benutzer von den einzelnen Instanzen des Treibers synchronisiert werden sollen. Mithilfe der Bereichsfilterung können Sie jedem Treiber Regeln hinzufügen, damit die Aktionen des Treibers auf bestimmte Container beschränkt werden. Siehe „Verwendung der Bereichsfilterung zum Verwalten von Benutzern auf verschiedenen Servern“, auf Seite 31.

- **Verwendung mehrerer Instanzen des Treibers auf mehreren Servern ohne Bereichsfilterung.** Wenn mehrere Instanzen eines Treibers auf mehreren Servern ohne die Verwendung gefilterter Reproduktionen laufen sollen, müssen Sie für die verschiedenen Treiberinstanzen Richtlinien definieren, auf deren Basis der Treiber im selben Identitätsdepot unterschiedliche Objektsätze verarbeiten kann.

- Die Schablonenobjekte, die vom Treiber bei der Erstellung von Benutzern verwendet werden sollen, sofern die Verwendung von Schablonen ausgewählt ist.

  Identity Manager-Treiber erfordern nicht, dass eDirectory-Schablonenobjekte für die Benutzererstellung festgelegt werden. Wenn Sie jedoch festlegen, dass ein Treiber eine Schablone für die Erstellung von Benutzern in eDirectory verwenden soll, muss das Schablonenobjekt auf dem Server repliziert werden, auf dem der Treiber läuft.

- Alle Container, die der Identity Manager-Treiber zur Benutzerverwaltung verwenden soll.

  Wenn Sie beispielweise einen Container namens „Inaktive Benutzer“ erstellt haben, der deaktivierte Benutzerkonten enthält, benötigen Sie eine Master- oder eine Lese-/Schreibreproduktion (vorzugsweise eine Masterreproduktion) für diesen Container auf dem Server, auf dem der Treiber läuft.

- Alle anderen Objekte, auf die sich der Treiber beziehen muss (z. B. Auftragsobjekte für den Avaya PBX-Treiber).

  Wenn die anderen Objekte vom Treiber nur gelesen und nicht geändert werden müssen, ist für diese Objekte auf dem Server eine Lesereproduktion ausreichend.

3.3.3 Verwendung der Bereichsfilterung zum Verwalten von Benutzern auf verschiedenen Servern

Mithilfe der Bereichsfilterung können Sie jedem Treiber Regeln hinzufügen, wodurch die Aktionen des Treibers auf bestimmte Container beschränkt werden. Die Bereichsfilterung sollte beispielsweise in den folgenden Situationen verwendet werden:

- Der Treiber soll nur die Benutzer in einem bestimmten Container synchronisieren.

  In der Standardeinstellung synchronisiert der Identity Manager-Treiber die Objekte in allen Containern, die auf dem Server repliziert sind, auf denen er läuft. Sie können diesen Bereich einschränken, indem Sie Regeln für die Bereichsfilterung erstellen.

- Ein Identity Manager-Treiber soll alle Benutzer synchronisieren, aber Sie möchten nicht, dass alle Benutzer auf demselben Server repliziert werden.

  Zur Synchronisierung von Benutzern, die nicht auf einem einzelnen Server repliziert sind, müssen Sie die Server festlegen, die alle Benutzer enthalten. Anschließend müssen Sie auf jedem dieser Server eine Instanz des Identity Manager-Treibers erstellen. Damit nicht zwei Instanzen

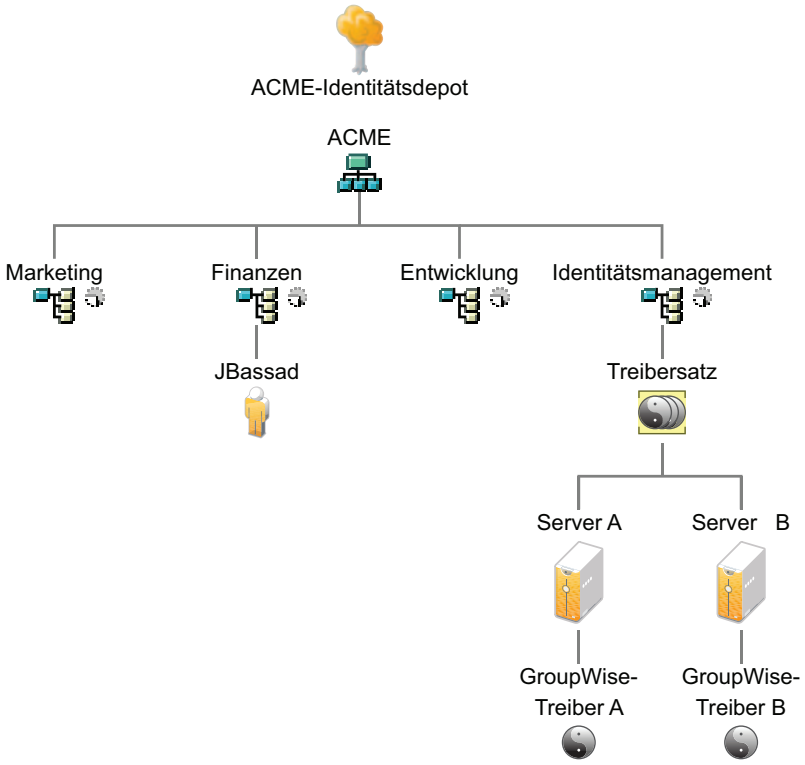
eines Treibers versuchen, dieselben Benutzer zu synchronisieren, müssen Sie in der Bereichsfilterung definieren, welche Benutzer von den einzelnen Instanzen des Treibers synchronisiert werden sollen.

Hinweis: Sie sollten die Bereichsfilterung auch dann verwenden, wenn sich die Reproduktionen der Server gegenwärtig nicht überschneiden. Es könnte sein, dass zu einem späteren Zeitpunkt Reproduktionen auf die Server übertragen werden, sodass eine unbeabsichtigte Überschneidung entsteht. Bei Verwendung der Bereichsfilterung versuchen die Identity Manager-Treiber nicht, dieselben Benutzer zu synchronisieren, selbst wenn zu einem späteren Zeitpunkt Reproduktionen auf die Server übertragen werden.

Im Folgenden finden Sie ein Beispiel für die Verwendung der Bereichsfilterung:

Die folgende Abbildung zeigt ein Identitätsdepot mit drei Containern, in denen folgende Benutzer gespeichert sind: „Marketing“, „Finanzen“ und „Entwicklung“. Sie zeigt auch einen Identitätsmanagement-Container, in dem die Treibersätze gespeichert sind. Jeder dieser Container ist eine separate Partition.

Abbildung 3-4 *Beispielbaum für die Bereichsfilterung*



In diesem Beispiel verfügt der Identity Manager-Administrator über zwei Identitätsdepot-Server, Server A und Server B (siehe Abbildung 3-5 auf Seite 33). Keiner der beiden Server enthält eine Kopie aller Benutzer. Jeder Server enthält zwei der drei Partitionen, sodass sich die auf den Servern gespeicherten Bereiche überschneiden.

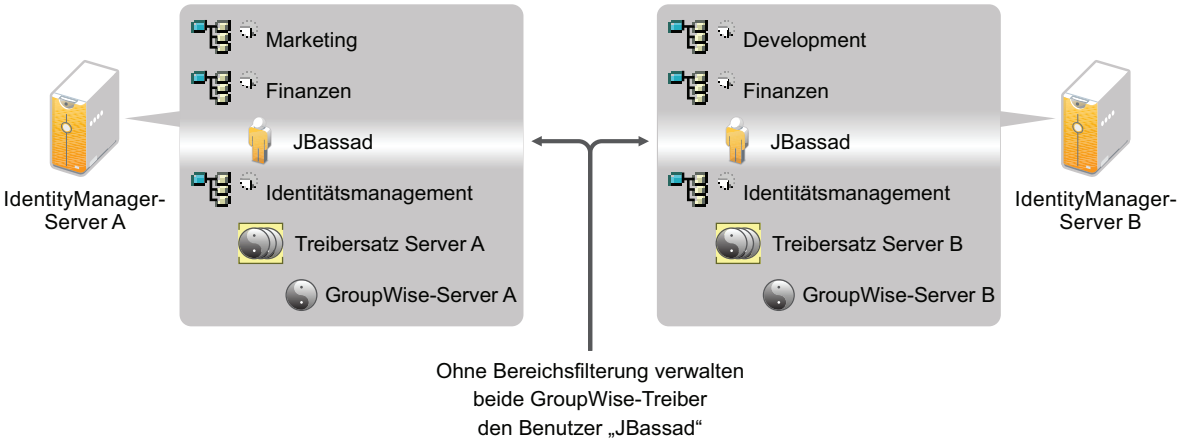
Der Administrator möchte, dass alle Benutzer im Baum vom GroupWise-Treiber synchronisiert werden, aber es sollen keine Reproduktionen der Benutzer auf einem einzelnen Server zusammengefasst werden. Stattdessen verwendet er zwei Instanzen des GroupWise-Treibers, von denen sich eine auf Server A, die andere auf Server B befindet. Er installiert Identity Manager und richtet auf beiden Identity Manager-Servern den GroupWise-Treiber ein.

Server A enthält Reproduktionen der Container „Marketing“ und „Finanzen“. Außerdem befindet sich auf dem Server eine Reproduktion des Identity Management-Containers, der den Treibersatz und das GroupWise-Treiberobjekt für Server A enthält.

Auf Server B befinden sich Reproduktionen der Container „Entwicklung“ und „Finanzen“ sowie der Identity Manager-Container, in dem sich der Treibersatz und das GroupWise-Treiberobjekt für Server B befinden.

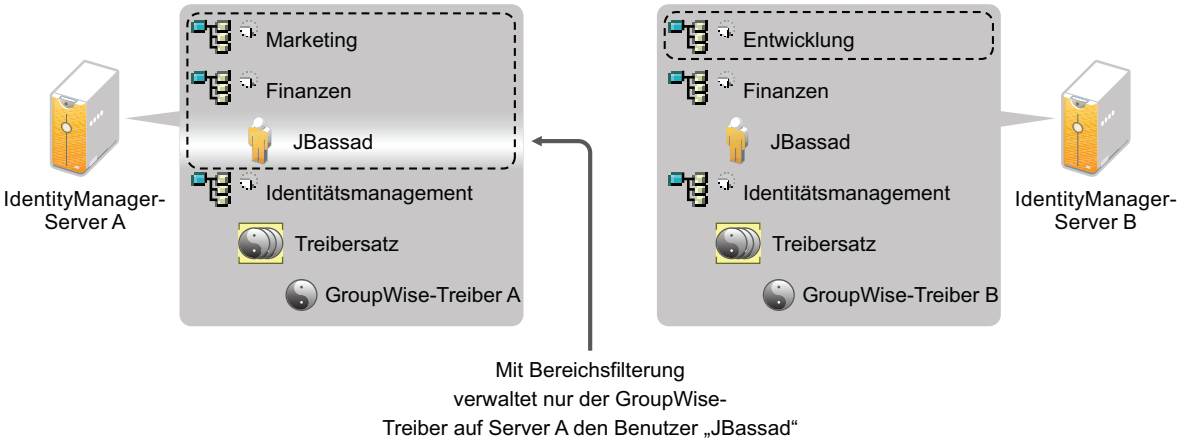
Da sich sowohl auf Server A als auch auf Server B eine Reproduktion des Containers „Finanzen“ befindet, ist auf beiden Servern der Benutzer „JBassad“ gespeichert, der sich im Container „Finanzen“ befindet. Ohne Bereichsfilterung nimmt sowohl GroupWise-Treiber A als auch GroupWise-Treiber B die Synchronisierung von „JBassad“ vor.

Abbildung 3-5 *Zwei Server mit sich überschneidenden Reproduktionen, ohne Bereichsfilterung.*



Die folgende Abbildung zeigt, dass durch die Bereichsfilterung verhindert wird, dass beide Instanzen des Treibers denselben Benutzer verwalten, weil definiert wird, welche Treiber die einzelnen Container synchronisieren.

Abbildung 3-6 *Die Bereichsfilterung definiert, welche Treiber die einzelnen Container synchronisieren*



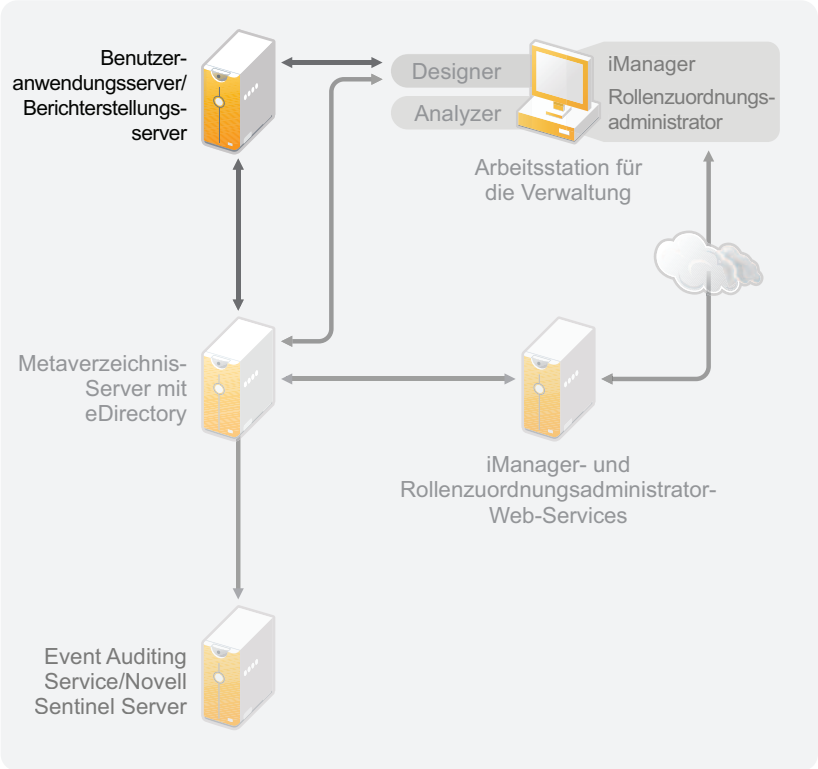
In Identity Manager sind vordefinierte Regeln enthalten. Zwei dieser Regeln dienen der Bereichsfilterung. Weitere Informationen zu den beiden Regeln “Ereignistransformation - Bereichsfilterung - Teilbäume einbeziehen” und “Ereignistransformation - Bereichsfilterung - Teilbäume ausschließen” finden Sie in *Richtlinien für Identity Manager 4.0.2*.

Für dieses Beispiel sollte die vordefinierte Regel „Teilbäume einbeziehen“ für Server A und Server B verwendet werden. Der Bereich muss für jeden Treiber unterschiedlich definiert sein, sodass sie nur die Benutzer in den angegebenen Containern synchronisieren. Server A würde die Container „Marketing“ und „Finanzen“ synchronisieren und Server B den Container „Entwicklung“.

3.4 Benutzeranwendung

Die Benutzeranwendung sollte auf einem separaten Server ausgeführt werden, wie in Abbildung 3-7 dargestellt. Sie benötigen möglicherweise mehrere Benutzeranwendungs-Server.

Abbildung 3-7 *Benutzeranwendung*

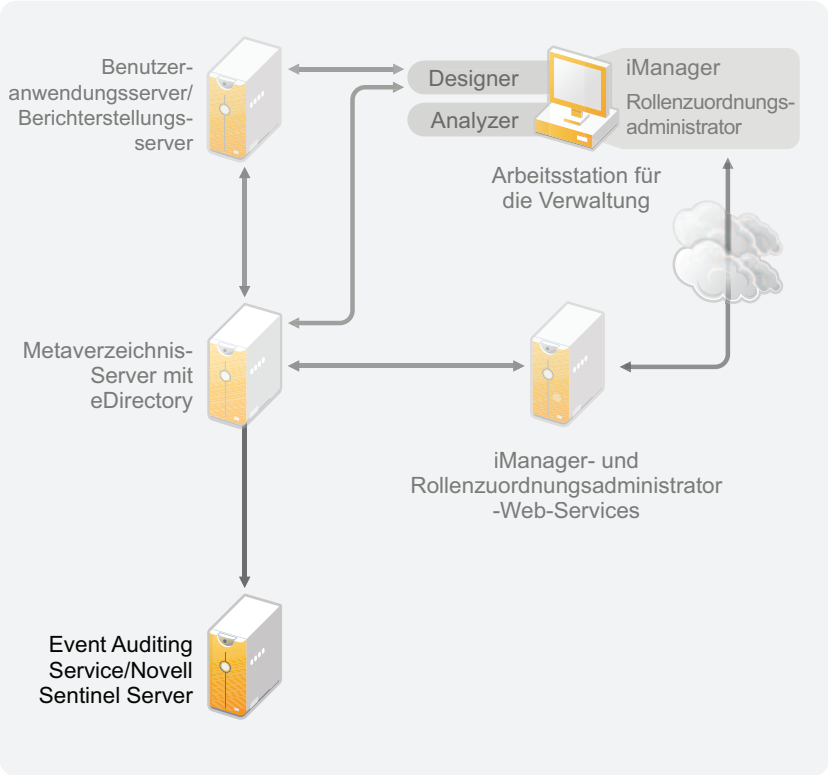


Anhand der Informationen im Abschnitt Leistungsoptimierung (http://www.novell.com/documentation/idmrbpm40/agpro/data/b2gx735.html) im *Benutzeranwendung: Verwaltungshandbuch* können Sie ermitteln, wie Sie den Benutzeranwendungs-Server am besten konfigurieren können.

3.5 Revision und Berichterstellung - Richtlinien

Wenn Sie als Teil der Identity Manager-Lösung Revisions- und Berichtsfunktionen benötigen, müssen Sie Identity Audit oder Novell Sentinel implementieren. Sie sollten entweder den Event Auditing Service oder Sentinel auf einem eigenen Server ausführen, wie in Abbildung 3-8 dargestellt. Die Anzahl der Server, die für Ihre Lösung erforderlich sind, hängt davon ab, über wie viele Treiber Sie in Ihrer Umgebung verfügen und wie viele Ereignisse Sie für die Revision definiert haben.

Abbildung 3-8 *Sentinel*



II Installation

Folgende Abschnitte enthalten die Informationen, die zur Installation eines Identity Manager-Systems ohne Verwendung des integrierten Installationsprogramms benötigt werden. Zum Vereinfachen der Installation und Konfiguration sollten Sie das neue integrierte Installationsprogramm nutzen, statt die Komponenten einzeln zu installieren. Weitere Informationen über das integrierte Installationsprogramm finden Sie im *Handbuch zur integrierten Installation von Identity Manager 4.0.2*.

Wenn Sie jedoch eine oder mehrere der Identity Manager-Komponenten einzeln installieren müssen, verwenden Sie zur Installation die Informationen in den folgenden Abschnitten.

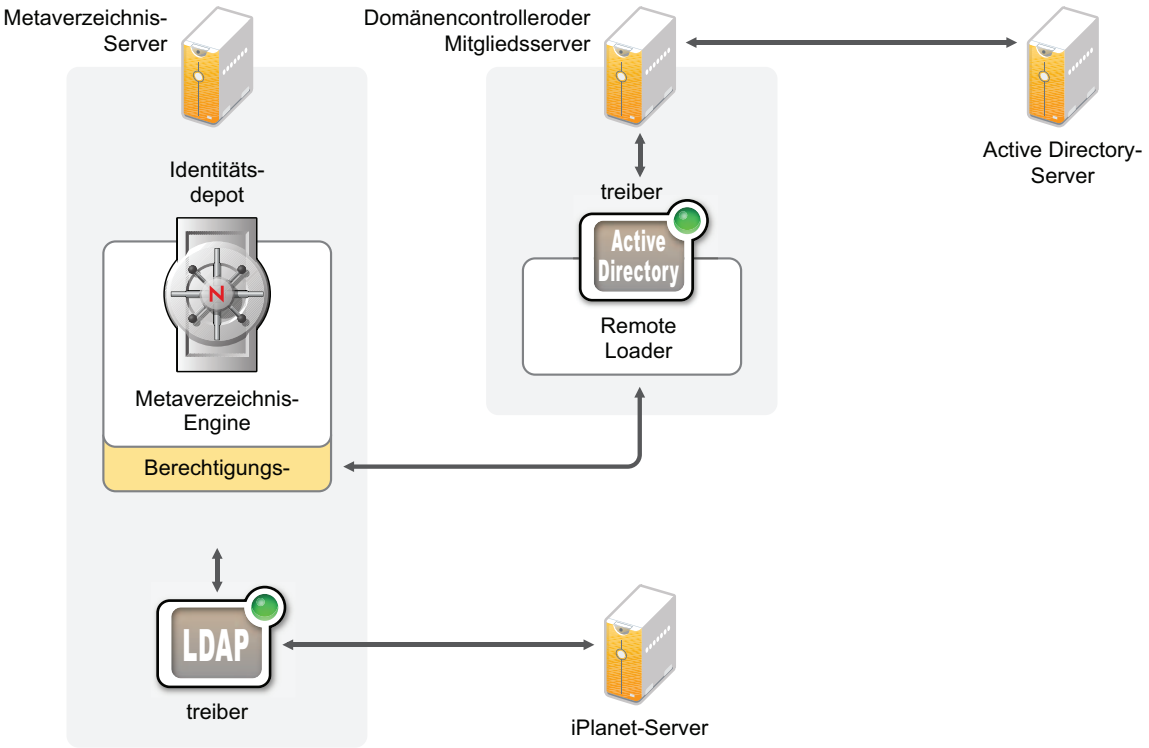
- Kapitel 4, „Basis-Checkliste für das Identity Manager-System“, auf Seite 39
- Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 43
- Kapitel 6, „Systemanforderungen“, auf Seite 47
- Kapitel 7, „Installation von Identity Manager“, auf Seite 63
- Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 81
- Kapitel 9, „Fehlerbehebung in Identity Manager“, auf Seite 85
- Kapitel 10, „Neue Funktionen“, auf Seite 93

4 Basis-Checkliste für das Identity Manager-System

Es gibt viele unterschiedliche Möglichkeiten, Identity Manager zu konfigurieren und alle Vorteile zu nutzen, die sich aus seinen Funktionen ergeben. Abbildung 4-1 stellt eine Basiskonfiguration von Identity Manager dar. Bei dieser Konfiguration erfolgt die Benutzerbereitstellung durch das Synchronisieren von Daten. Unabhängig von der Identity Manager-Konfiguration beginnen Sie immer mit einem Basissystem.

Anhand dieser Checkliste können Sie Ihr Identity Manager-System konfigurieren und dabei sicherstellen, dass alle Schritte vollständig ausgeführt werden.

Abbildung 4-1 *Identity Manager-Basissystem*



- Abschnitt 4.1, „Voraussetzungen“, auf Seite 40
- Abschnitt 4.2, „Planung“, auf Seite 40
- Abschnitt 4.3, „Installation“, auf Seite 40
- Abschnitt 4.4, „Treiberkonfiguration mit dem Remote Loader“, auf Seite 41
- Abschnitt 4.5, „Treiberkonfiguration ohne den Remote Loader“, auf Seite 41
- Abschnitt 4.6, „Zusätzliche Konfiguration“, auf Seite 42

4.1 Voraussetzungen

- ❒ Vergewissern Sie sich, dass Ihr System die unter Kapitel 6, „Systemanforderungen“, auf Seite 47 aufgeführten Systemanforderungen erfüllt.

4.2 Planung

Eine sorgfältige Planung ist der Schlüssel für eine erfolgreiche Implementierung und Bereitstellung von Identity Manager.

- ❒ Erstellen Sie eine Entwicklungsumgebung. Es ist wichtig, über Zugriff auf ein Identity Manager-System zu verfügen, damit Sie Ihre Identity Manager-Lösung validieren können. Sie sollten alle Tests und die Entwicklung in der Entwicklungsumgebung durchführen, bevor Sie zur Produktionsumgebung wechseln. Weitere Informationen finden Sie in Kapitel 1, „Einrichten einer Entwicklungsumgebung“, auf Seite 11.
- ❒ Erstellen Sie einen Projektplan für die Bereitstellung von Identity Manager. Zu den Aufgaben beim Erstellen eines Projektplans gehören das Definieren der wesentlichen Geschäftsprozesse, das Erstellen einer Identity Manager-Lösung, die diese Prozesse automatisiert, und das Erstellen eines Plans zur technischen Implementierung. Sie benötigen unbedingt einen Projektplan, damit Identity Manager erfolgreich bereitgestellt werden kann. Weitere Informationen finden Sie in Kapitel 2, „Erstellen eines Projektplans“, auf Seite 13.
- ❒ Nachdem Sie einen Projektplan erstellt haben, verwenden Sie Analyzer, um die Daten für die Synchronisierung zu bereinigen und vorzubereiten. Weitere Informationen hierzu finden Sie im *Analyzer 4.0.2 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.1 für Identity Manager).

4.3 Installation

- ❒ Installieren Sie Analyzer. Weitere Informationen finden Sie in Abschnitt 7.1, „Installation von Analyzer“, auf Seite 63.
- ❒ Installieren Sie Designer. Weitere Informationen finden Sie in Abschnitt 7.2, „Installation von Designer“, auf Seite 64.
- ❒ Installieren Sie eDirectory. Weitere Informationen finden Sie in Abschnitt 7.3, „Installieren von eDirectory“, auf Seite 65.
- ❒ Installieren Sie iManager. Weitere Informationen finden Sie in Abschnitt 7.4, „Installieren von iManager“, auf Seite 66.
- ❒ Installieren Sie den Metaverzeichnis-Server und -Treiber. Weitere Informationen finden Sie in Kapitel 7, „Installation von Identity Manager“, auf Seite 63.
- ❒ Aktivieren Sie Identity Manager. Weitere Informationen finden Sie in Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 81.
- ❒ (Optional) Entwerfen und erstellen Sie Berechtigungen für Ihr Identity Manager-System.

  Berechtigungen sind definierte Kriterien für eine Person oder Gruppe, die auf mehrere Treiber angewendet werden können. Werden die Kriterien erfüllt, initiieren die Berechtigungen ein Ereignis zum Erteilen oder Entziehen von Zugriffsrechten auf Geschäftsressourcen. Berechtigungen bieten zusätzliche Steuerungs- und Automatisierungsmöglichkeiten zum Erteilen und Entziehen von Zugriffsrechten auf Ressourcen.

Der wesentliche Vorteil von Berechtigungen besteht darin, dass man Geschäftslogik erstellen bzw. definieren und diese Logik dann auf mehrere Treiber anwenden kann. Wenn Sie eine Änderung vornehmen müssen, nehmen Sie diese in der Berechtigung vor und nicht in den einzelnen Treibern.

Berechtigungen werden anhand der folgenden drei Agenten implementiert:

- Rollenbasierte Berechtigungen mithilfe des Berechtigungsservice-Treibers
- Workflow
- Rollenbasiertes Bereitstellungsmodul

Weitere Informationen zu Berechtigungen finden Sie im *Identity Manager 4.0.2 Entitlements Guide* (Handbuch zu Identity Manager 4.0.1 Berechtigungen).

4.4 Treiberkonfiguration mit dem Remote Loader

Der Remote Loader ermöglicht das Synchronisieren von Informationen zu einem verbundenen System, ohne dass eDirectory auf diesem verbundenen System installiert sein muss. Der Remote Loader synchronisiert die Informationen auf den Metaverzeichnis-Server, der die Daten im Identitätsdepot speichert. Identity Manager verwendet eDirectory als Identitätsdepot.

- ❒ Installieren Sie den Remote Loader auf einem Computer, der mit dem verbundenen System kommuniziert. Der Remote Loader kommuniziert zwischen dem verbundenen System und dem Metaverzeichnis-Server. Er ermöglicht die Kommunikation von Identity Manager mit einem Computer, auf dem eDirectory nicht installiert ist. Weitere Informationen hierzu finden Sie unter "Installing the Remote Loader" (Installation des Remote Loaders) im *Identity Manager 4.0.2 Remote Loader Guide* (Handbuch zu Identity Manager 4.0.1 Remote Loader).
- ❒ Konfigurieren Sie den Remote Loader für einen Treiber. Sie definieren eine bestimmte Instanz von Remote Loader für die Kommunikation mit einem bestimmten Treiber. Weitere Informationen hierzu finden Sie unter "Configuring the Remote Loader" (Konfigurieren des Remote Loaders) im *Identity Manager 4.0.2 Remote Loader Guide* (Handbuch zu Identity Manager 4.0.1 Remote Loader).
- ❒ Konfigurieren Sie den Treiber für die Kommunikation mit dem Remote Loader. Für jeden Treiber steht ein Treiberhandbuch zur Verfügung. Spezielle Informationen zu Ihrem Treiber finden Sie auf der Website zur Identity Manager 4.0.2 Treiber-Dokumentation (http://www.novell.com/documentation/idm402drivers/).
- ❒ (Optional) Aktivieren Sie die Berechtigungen auf dem Treiber. Vergewissern Sie sich, dass die korrekten Richtlinien zum Ausführen der Berechtigung aktiv sind. Weitere Informationen finden Sie im *Identity Manager 4.0.2 Entitlements Guide* (Handbuch zu Identity Manager 4.0.1 Berechtigungen).
- ❒ Wiederholen Sie diese Schritte für jeden Treiber in Ihrer Umgebung.

4.5 Treiberkonfiguration ohne den Remote Loader

- ❒ Erstellen und konfigurieren Sie Ihren Treiber. Für jeden Treiber steht ein Treiberhandbuch zur Verfügung. Spezielle Informationen zu Ihrem Treiber finden Sie auf der Website zur Identity Manager 4.0.2 Treiber-Dokumentation (http://www.novell.com/documentation/idm402drivers/).

- ❒ (Optional) Aktivieren Sie die Berechtigungen auf dem Treiber. Vergewissern Sie sich, dass die korrekten Richtlinien zum Ausführen der Berechtigung aktiv sind. Weitere Informationen finden Sie im *Identity Manager 4.0.2 Entitlements Guide* (Handbuch zu Identity Manager 4.0.1 Berechtigungen).
- ❒ Wiederholen Sie diese Schritte für jeden Treiber in Ihrer Umgebung.

4.6 Zusätzliche Konfiguration

Wenn das Identity Manager-Basissystem installiert und konfiguriert ist, können Sie die folgenden zusätzlichen Konfigurationsaufgaben durchführen:

- ❒ **Passwortverwaltung:** Wenn Sie Passwörter mit Identity Manager verwalten möchten, müssen Sie einige zusätzliche Einstellungen vornehmen. Verwenden Sie die "Checkliste für die Passwortverwaltung" im *Identity Manager 4.0.2 Password Management Guide* (Handbuch zur Identity Manager 4.0.1 Passwortverwaltung), um zu überprüfen, ob alle Konfigurationsschritte vollständig ausgeführt wurden.
- ❒ **Rollenverwaltung:** Wenn Sie Rollen von einem Standort aus über verschiedene Systeme hinweg verwalten möchten, können Sie den in Identity Manager enthaltenen Rollenzuordnungsadministrator verwenden. Dieser ermöglicht Ihnen die Zuordnung von Geschäftsrollen von einem System zu einem anderen, ohne dass Sie die IT-Infrastruktur kennen müssen. Weitere Informationen finden Sie im *Identity Manager Role Mapping Administrator 4.0.2 Installation and Configuration Guide* (Installations- und Konfigurationshandbuch zum Identity Manager-Rollenzuordnungsadministrator 4.0).
- ❒ **Rollenbasierte Bereitstellung:** Wenn Sie die rollenbasierte Bereitstellung in Ihre Identity Manager-Lösung einbinden möchten, verwenden Sie die "Installations-Checkliste" im *Identity Manager Roles Based Provisioning Module 4.0.2 User Application: Installation Guide* (Rollenbasiertes Bereitstellungsmodul für Identity Manager 4.0.1 Benutzeranwendung: Installationshandbuch), um sicherzustellen, dass alle Konfigurationsschritte ausgeführt wurden.
- ❒ **Revision und Berichterstellung:** Die Verwendung der Revisions- und Berichterstellungsfunktionen in Ihrer Identity Manager-Lösung ist ein Mittel, mit dem Sie zeigen können, dass Ihre Geschäftsrichtlinien mit den Firmenrichtlinien übereinstimmen. Für Revisionen und Berichterstellung können Sie das Identitätsberichterstellungsmodul oder Novell Sentinel in Ihre Identity Manager-Lösung integrieren. Weitere Informationen hierzu finden Sie im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul). Weitere Informationen zu Novell Sentinel finden Sie im *Identity Manager 4.0.2 Reporting Guide for Novell Sentinel* (Identity Manager 4.0.1 Berichtshandbuch für Novell Sentinel).

5 Bezugsquellen für Identity Manager

Identity Manager 4.0.2 ist in den Ausführungen „Advanced“ und „Standard“ verfügbar. Es gibt separate ISO-Imagedateien für jede Ausführung. Die Identity Manager 4.0.2 Advanced Edition enthält einen vollständigen Satz an Funktionen der Unternehmensklasse zur Bereitstellung von Benutzern. Um die verschiedenen Anforderungen der Kunden zu erfüllen, enthält die Identity Manager Standard Edition einen Teil der Funktionen, die in der Identity Manager Advanced Edition verfügbar sind. Die Standard Edition bietet auch weiterhin alle Funktionen, die in älteren Versionen von Identity Manager vorhanden sind. Weitere Informationen zum Funktionsumfang der Identity Manager 4.0.2 Advanced und Standard Edition finden Sie unter “Identity Manager 4.0.2 Funktionen ” im *Identity Manager 4.0.2 Overview Guide* (Identity Manager 4.0.1 Übersichtshandbuch).

Sie können eine Testversion von Identity Manager herunterladen und 90 Tage lang kostenlos nutzen. Die Komponenten von Identity Manager müssen jedoch innerhalb von 90 Tagen nach der Installation aktiviert werden, anderenfalls wird ihre Funktion eingestellt. Sie können Identity Manager zu einem beliebigen Zeitpunkt während oder nach Ablauf der 90 Tage durch den Kauf einer Produktlizenz aktivieren. Weitere Informationen finden Sie in Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 81.

So können Sie Identity Manager und -Services herunterladen:

1. Rufen Sie die Download-Website von Novell (http://download.novell.com) auf.
2. Wählen Sie im Menü *Produkt oder Technologie* den Eintrag *Identity Manager* aus und klicken Sie auf *Suchen*.
3. Klicken Sie auf der Download-Website von Novell Identity Manager auf die Schaltfläche *Download* neben der gewünschten Datei. Tabelle 5-1 enthält eine Beschreibung zu jeder Datei.

   Sie können eine entsprechende ISO-Imagedatei gemäß Ihren Anforderungen auswählen. Jede ISO-Imagedatei enthält die 32-Bit- und 64-Bit-Version des Produkts.

   Wichtig: Wenn Sie von der Identity Manager Advanced Edition zur Standard Edition wechseln möchten, deinstallieren Sie die Advanced Edition und installieren Sie dann die Standard Edition-ISO-Imagedatei von dem Identity Manager-Medium. Wenn Sie von der Standard Edition zur Advanced Edition aufrüsten möchten, verwenden Sie die Identity Manager Advanced Edition-ISO-Imagedatei. Sie müssen die richtige Aktivierung anwenden, um auf die Advanced Edition aufrüsten zu können. Weitere Informationen zum Aufrüsten von der Standard Edition auf die Advanced Edition finden Sie im *Identity Manager 4.0.2 Aufrüstungs- und Migrationshandbuch*.
4. Befolgen Sie die Bildschirmanweisungen, um die Datei in einen Ordner auf Ihrem Computer herunterzuladen.
5. Wiederholen Sie Schritt 3, bis Sie alle erforderlichen Dateien heruntergeladen haben.
6. Mounten Sie die heruntergeladene `.iso`-Datei als Volume oder verwenden Sie die `.iso`-Datei zum Erstellen einer DVD der Software. Wenn Sie noch nicht geprüft haben, ob der gebrannte Datenträger gültig ist, können Sie dies mit Hilfe der Option *Medienprüfung* tun.

Hinweis: Die Linux ISO-Dateien sollten aufgrund der Größe der Dateien auf eine Doppel-DVD kopiert werden.

Tabelle 5-1 *Identity Manager-ISO-Imagedateien*

ISO	Plattform	Beschreibung
`Identity_Manager_4.0.2_Windows_Advanced.iso`	Windows	Enthält das DVD-Image für den Metaverzeichnis-Server, Designer, iManager, Rollenzuordnungsadministrator, Analyzer, das Identitätsberichterstellungsmodul und das rollenbasierte Bereitstellungsmodul.
`Identity_Manager_4.0.2_Windows_Standard.iso`	Windows	Enthält das DVD-Image für den Metaverzeichnis-Server, Designer, iManager, Analyzer, das Identitätsberichterstellungsmodul und das rollenbasierte Bereitstellungsmodul.
`Identity_Manager_4.0.2_Linux_Advanced.iso`	Linux	Enthält das DVD-Image für den Metaverzeichnis-Server, Designer, iManager, Rollenzuordnungsadministrator, Analyzer, das Identitätsberichterstellungsmodul und das rollenbasierte Bereitstellungsmodul.
`Identity_Manager_4.0.2_Linux_Standard.iso`	Linux	Enthält das DVD-Image für den Metaverzeichnis-Server, Designer, iManager, Analyzer, das Identitätsberichterstellungsmodul und das rollenbasierte Bereitstellungsmodul.
`Identity_Manager_4.0.2_Solaris_Advanced.iso`	Solaris	Enthält das DVD-Image für den Metaverzeichnis-Server. Andere Komponenten werden auf der Solaris-Plattform nicht unterstützt.
`Identity_Manager_4.0.2_Solaris_Standard.iso`	Solaris	Enthält das DVD-Image für den Metaverzeichnis-Server. Andere Komponenten werden auf der Solaris-Plattform nicht unterstützt.

Mit dem Kauf von Identity Manager haben Sie auch Aktivierungen für Service-Treiber und verschiedene allgemeine Treiber erworben.

- **Service-Treiber:** Folgende Liste enthält die Service-Treiber, die aktiviert werden, wenn Sie den Metaverzeichnis-Server aktivieren:
  - Datenerfassungsdienst
  - Berechtigungsservices
  - ID-Provider
  - Loopback-Service
  - Verwaltetes System - Gateway
  - 'Manuelle Aufgabe'-Service
  - Null-Service
  - Rollen- und Ressourcenservice
  - Benutzeranwendung
  - Auftrag

- **Allgemeine Treiber:** Folgende Liste enthält die allgemeinen Treiber, die aktiviert werden, wenn Sie den Metaverzeichnis-Server aktivieren:
  - Active Directory
  - ADAM
  - eDirectory
  - GroupWise
  - LDAP
  - Lotus Notes

Aktivierungen für alle anderen Identity Manager-Treiber müssen separat erworben werden. Die Aktivierungen für die Treiber sind als Identity Manager-Integrationsmodule erhältlich. Ein Identity Manager-Integrationsmodul kann einen oder mehrere Treiber enthalten. Sie erhalten für jedes erworbene Identity Manager-Integrationsmodul eine Produktaktivierungsberechtigung. Weitere Informationen hierzu finden Sie auf der Webseite für Identity Manager-Treiberprodukte (http://www.novell.com/products/identitymanager/drivers/).

Für die Identity Manager Advanced Edition und die Standard Edition sind jeweils eigene Aktivierungsschlüssel verfügbar. Weitere Informationen hierzu finden Sie in „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 81. Ein Wechsel von der Identity Manager Advanced Edition zur Standard Edition ohne Neuinstallion wird nicht unterstützt. Wenn Sie die Identity Manager Standard Edition verwenden möchten, müssen Sie sie vom Identity Manager-Medium installieren.

Das rollenbasierte Bereitstellungsmodul der Benutzeranwendung ist im Lieferumfang von Identity Manager enthalten. Es ermöglicht einen leistungsstarken rollenbasierten Genehmigungs-Workflow für die Verwaltung der Identitäten Ihrer Benutzer.

Identity Manager umfasst des Weiteren verschiedene Werkzeuge zum Gestalten, Erstellen und Verwalten Ihrer Identity Manager-Lösung:

- Analyzer
- Designer
- iManager
- Rollenzuordnungsadministrator

Hinweis: Der Rollenzuordnungsadministrator ist in der Identity Manager 4.0.2 Standard Edition nicht verfügbar.

Das Identitätsberichterstellungsmodul ist eine weitere Komponente von Identity Manager, mit der Sie Berichte zu Ihrer Identity Manager-Lösung prüfen und erstellen können. Die Berichte können Ihnen dabei helfen, die Einhaltung etwaiger für Ihre Branche geltender Vorschriften zu gewährleisten.

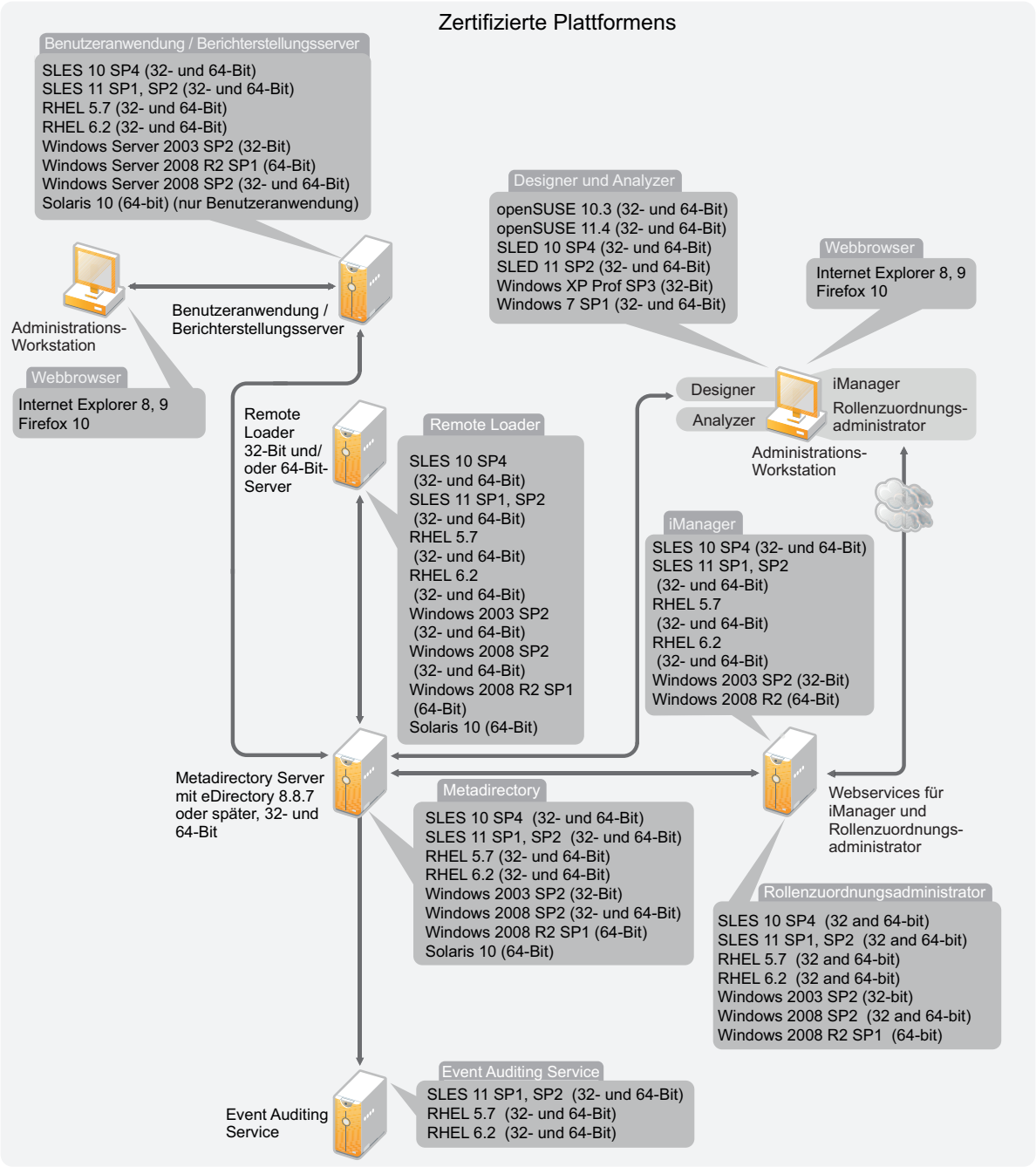
Weitere Informationen über die Identity Manager-Komponenten finden Sie im *Identity Manager 4.0.2 Overview Guide* (Identity Manager 4.0.1 Übersichtshandbuch).

6 Systemanforderungen

Sie können Komponenten von Novell Identity Manager auf verschiedenen Systemen und Plattformen installieren.

Abbildung 6-1 zeigt, welche Plattformen und Systeme unterstützt werden.

Abbildung 6-1 *Systemanforderungen für die Identity Manager-Komponenten*



Je nach Systemkonfiguration müssen Sie das Identity Manager-Installationsprogramm möglicherweise mehrmals ausführen, um die Komponenten von Identity Manager auf den entsprechenden Systemen zu installieren.

Abhängige Bibliotheken für die Installation von Identity Manager auf RHEL 6.0

Vor der Installation von Identity Manager auf RHEL 6.0 müssen Sie auf jeden Fall die folgenden Bibliotheken installieren:

- **Zur GUI-Installation:** Vor der Aktivierung des Installationsprogramms für Identity Manager müssen die abhängigen Bibliotheken manuell installiert werden.
  - **Für ein 64-Bit-RHEL:** Installieren Sie die folgenden Bibliotheken in der angegebenen Reihenfolge:
    1. `libXau-1.0.5-1.el6.i686.rpm`
    2. `libxcb-1.5-1.el6.i686.rpm`
    3. `libX11-1.3-2.el6.i686.rpm`
    4. `libXext-1.1-3.el6.i686.rpm`
    5. `libXi-1.3-3.el6.i686.rpm`
    6. `libXtst-1.0.99.2-3.el6.i686.rpm`
    7. `glibc-2.12-1.7.el6.i686.rpm`
    8. `libstdc++-4.4.4-13.el6.i686.rpm`
    9. `libgcc-4.4.4-13.el6.i686.rpm`
    10. `compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm`
    11. `compat-libstdc++-33-3.2.3-69.el6.i686.rpm`
  - **Für ein 32-Bit-RHEL:** Installieren Sie die folgende Bibliothek:
    - `compat-libstdc++-33-3.2.3-69.el6.i686.rpm`
- **Zur Installation ohne GUI:** Vor der Aktivierung des Installationsprogramms für Identity Manager müssen die abhängigen Bibliotheken manuell installiert werden.
  - **Für ein 64-Bit-RHEL:** Installieren Sie die folgenden Bibliotheken in der angegebenen Reihenfolge:
    1. `glibc-2.12-1.7.el6.i686.rpm`
    2. `libstdc++-4.4.4-13.el6.i686.rpm`
    3. `libgcc-4.4.4-13.el6.i686.rpm`
    4. `compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm`
    5. `compat-libstdc++-33-3.2.3-69.el6.i686.rpm`
  - **Für ein 32-Bit-RHEL:** Installieren Sie die folgende Bibliothek:
    - `compat-libstdc++-33-3.2.3-69.el6.i686.rpm`

Hinweis: Vor der Installation von Identity Manager muss auf jeden Fall die `unzip`-RPM installiert sein. Dies gilt für alle Linux-Plattformen.

In den folgenden Abschnitten finden Sie die Systemanforderungen für Identity Manager-Komponenten:

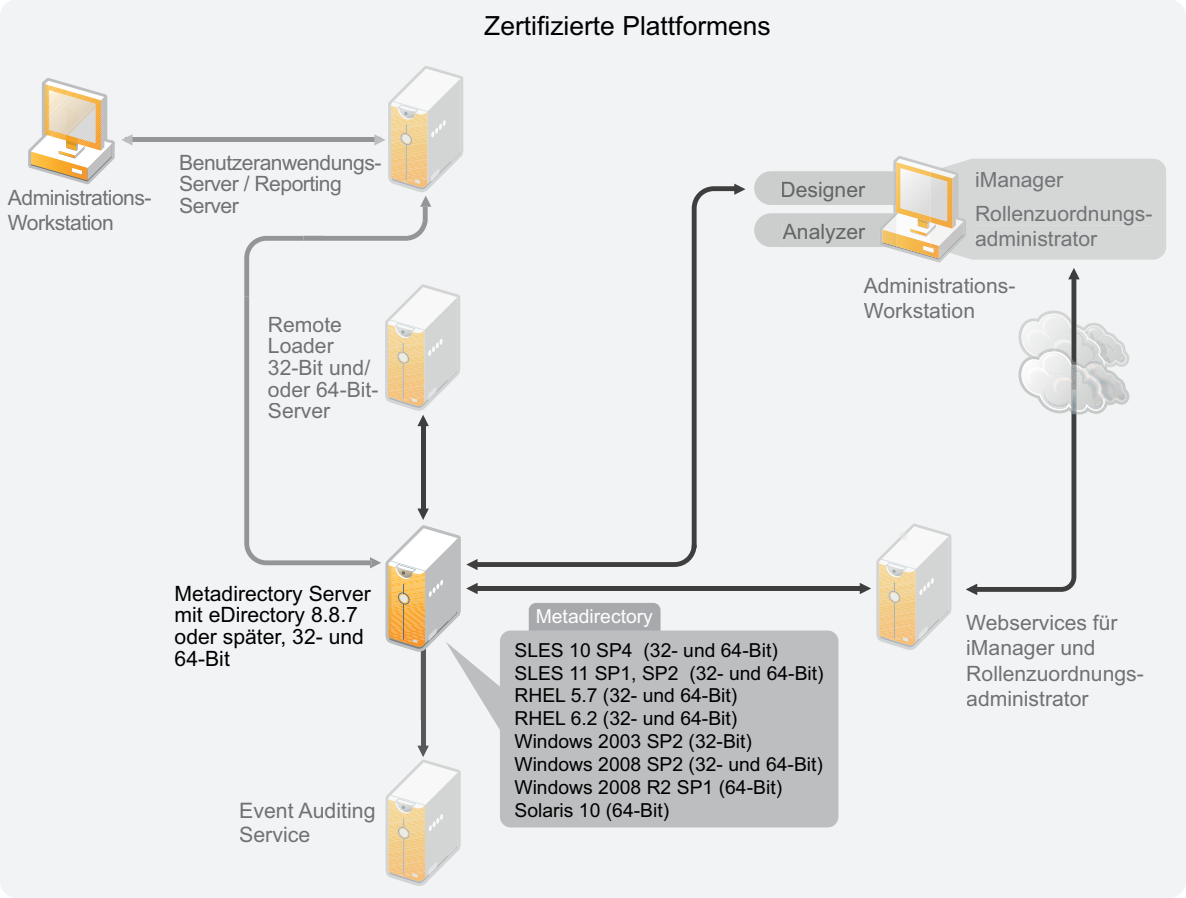
- Abschnitt 6.1, „eDirectory und iManager“, auf Seite 50
- Abschnitt 6.2, „Metaverzeichnis-Server“, auf Seite 51
- Abschnitt 6.3, „Remote Loader“, auf Seite 54
- Abschnitt 6.4, „Benutzeranwendung“, auf Seite 57

- Abschnitt 6.5, „Revision und Berichterstellung“, auf Seite 57
- Abschnitt 6.6, „Arbeitsstationen“, auf Seite 59
- Abschnitt 6.7, „Ressourcenanforderungen“, auf Seite 61

6.1 eDirectory und iManager

Für Identity Manager wird vorausgesetzt, dass eDirectory und iManager installiert sind. Diese Produkte bieten eine Basis für Identity Manager und sind in der ISO-Imagedatei der Identity Manager Advanced Edition enthalten. Abbildung 6-2 veranschaulicht diese Komponenten.

Abbildung 6-2 *Basisprodukte für Identity Manager*



Sie benötigen folgende Versionen dieser Produkte:

- eDirectory 8.8.7 oder höher (32 oder 64 Bit)

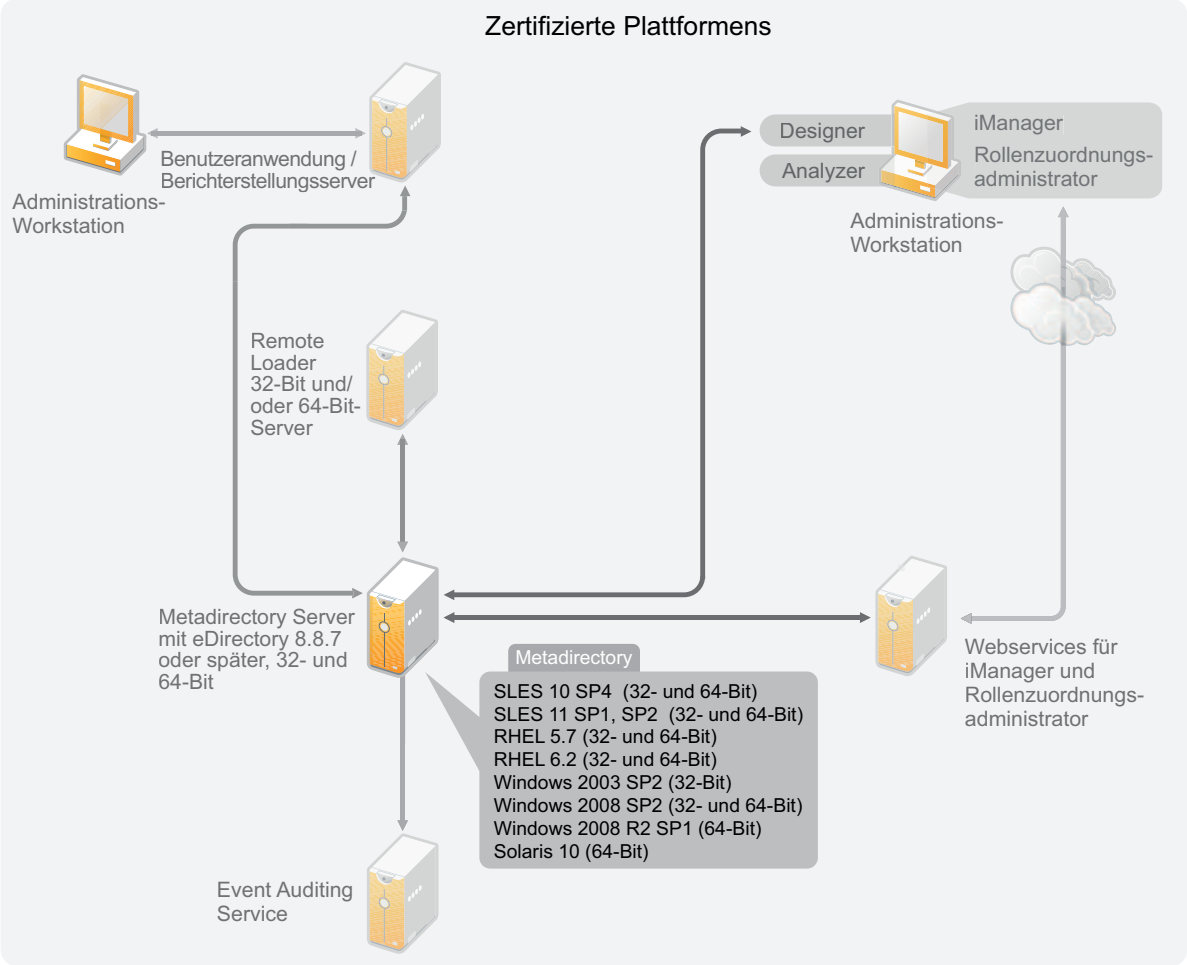
  Informationen zu den Systemanforderungen für eDirectory finden Sie im *Novell eDirectory 8.8 Installation Guide* (http://www.novell.com/documentation/edir88/index.html) (Novell eDirectory 8.8 Installationshandbuch).

- iManager 2.7.5

6.2 Metaverzeichnis-Server

Der Metaverzeichnis-Server verarbeitet die Treiberereignisse - und zwar unabhängig davon, ob sie mit dem Remote Loader konfiguriert wurden oder nicht. Eine Liste der unterstützten Betriebssysteme finden Sie in Abbildung 6-3.

Abbildung 6-3 *Unterstützte Betriebssysteme für den Metaverzeichnis-Server*



Während der Installation des Metaverzeichnis-Servers erkennt das Installationsprogramm, welche eDirectory-Version installiert ist.

Hinweis: Auf dem Computer muss eDirectory 8.8.7 oder höher (32 oder 64 Bit) installiert sein. Ist dies nicht der Fall, wird die Installation abgebrochen.

- Abschnitt 6.2.1, „Unterstützte Prozessoren“, auf Seite 52
- Abschnitt 6.2.2, „Server-Betriebssysteme“, auf Seite 52

6.2.1 Unterstützte Prozessoren

Die hier aufgelisteten Prozessoren werden zum Testen von Identity Manager verwendet. Der SPARC-Prozessor wird für Solaris-Tests verwendet.

Folgende 32-Bit-Prozessoren werden für Linux- (Red Hat und SUSE Linux Enterprise Server) und Windows-Betriebssysteme unterstützt:

- Intel x86-32
- AMD x86-32

Folgende 64-Bit-Prozessoren werden für Linux- (Red Hat und SUSE Linux Enterprise Server) und Windows-Betriebssysteme unterstützt:

- Intel EM64T
- AMD Athlon64
- AMD Opteron

Es sollten die neuesten Support-Packs für alle Betriebssysteme installiert sein.

6.2.2 Server-Betriebssysteme

Sie können den Metaverzeichnis-Server als 32-Bit-Anwendung auf einem 64-Bit-Betriebssystem installieren. Tabelle 6-1 enthält eine Liste der zertifizierten und unterstützten Server-Betriebssysteme, auf denen der Metaverzeichnis-Server ausgeführt werden kann.

Wichtig: Unter einer zertifizierten Plattform versteht man eine Plattform, die vollständig getestet wurde. Eine unterstützte Plattform wurde zwar nicht getestet, es wird aber erwartet, dass sie voll funktionsfähig ist.

Tabelle 6-1 *Zertifizierte und unterstützte Server-Betriebssysteme*

Version des Server-Betriebssystems	Zertifiziert	Unterstützt	Haftnotizen
Windows Server 2003 SP2 (32 Bit)	Ja	Unterstützt auf neueren Versionen von Service Packs	Der Metaverzeichnis-Server läuft nur im 32-Bit-Modus.
Support-Pakete für Windows 2008 SP1 oder höher (32 Bit und 64 Bit)	Ja	Unterstützt auf neueren Versionen von Service Packs	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus.
Windows Server 2008 R2 (64 Bit)	Ja	Ja	Der Metaverzeichnis-Server läuft nur im 64-Bit-Modus.

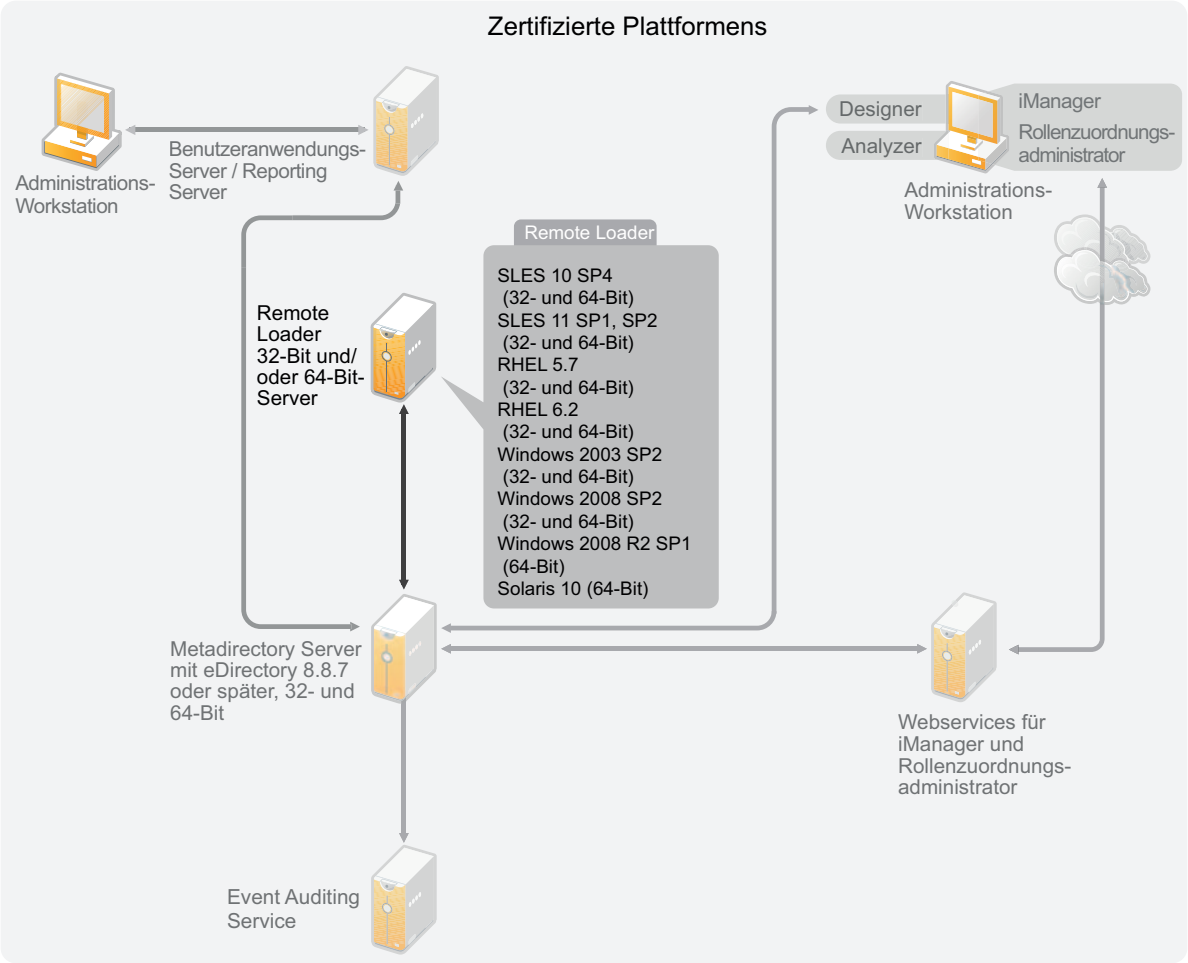
Version des Server-Betriebssystems	Zertifiziert	Unterstützt	Haftnotizen
Red Hat 5.7 (32 Bit und 64 Bit)	Ja	Unterstützt auf neueren Versionen von Support-Paketen	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus. Novell empfiehlt, dass Sie vor der Installation von Identity Manager mit der automatischen Aktualisierungsfunktion des Herstellers die neuesten Betriebssystem-Patches aufspielen.
Red Hat 6.0 (32 Bit und 64 Bit)	Zertifiziert für Red Hat 6.2	Unterstützt auf neueren Versionen von Support-Paketen	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus. Novell empfiehlt, dass Sie vor der Installation von Identity Manager mit der automatischen Aktualisierungsfunktion des Herstellers die neuesten Betriebssystem-Patches aufspielen.
SUSE Linux Enterprise Server 10 SP4 (32 Bit und 64 Bit)	Ja	Unterstützt auf neueren Versionen von Support-Paketen	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus. Novell empfiehlt, dass Sie vor der Installation von Identity Manager mit der automatischen Aktualisierungsfunktion des Herstellers die neuesten Betriebssystem-Patches aufspielen.
SUSE Linux Enterprise Server 11 SP1 (32 Bit und 64 Bit)	Ja	Unterstützt auf neueren Versionen von Support-Paketen	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus. Novell empfiehlt, dass Sie vor der Installation von Identity Manager mit der automatischen Aktualisierungsfunktion des Herstellers die neuesten Betriebssystem-Patches aufspielen.
SUSE Linux Enterprise Server 11 SP2 (32 Bit und 64 Bit)	Ja	Ja	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus. Novell empfiehlt, dass Sie vor der Installation von Identity Manager mit der automatischen Aktualisierungsfunktion des Herstellers die neuesten Betriebssystem-Patches aufspielen.
OES 2 SP3 (32 Bit und 64 Bit)	Ja	Ja	Der Metaverzeichnis-Server läuft im 32-Bit- und im 64-Bit-Modus.

Version des Server-Betriebssystems	Zertifiziert	Unterstützt	Haftnotizen
OES 11 SP1 oder höher (64 Bit)	Ja	Ja	Der Metaverzeichnis-Server läuft nur im 64-Bit-Modus.
Solaris 10 (64 Bit)	Ja	Ja	Der Metaverzeichnis-Server läuft nur im 64-Bit-Modus.
Xen	Ja	Ja	Xen wird unterstützt, wenn die Xen Virtual Machine als Gastbetriebssystem entweder SLES 10 oder SLES 11 im paravirtualisierten Modus ausführt.
VMware ESX und ESXi 4.0	Ja	Ja	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus.
VMware ESXi-Arbeitsstation	Ja	Ja	
Red Hat Enterprise Linux 5 Virtualisierung	Nein	Ja	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus.
Windows Server 2008 R2 Virtualisierung mit Hyper-V	Nein	Ja	Der Metaverzeichnis-Server läuft entweder im 32-Bit- oder im 64-Bit-Modus.

6.3 Remote Loader

Der Remote Loader gibt Ihnen mehr Flexibilität bei der Konfiguration Ihrer Identity Manager-Lösung. Er unterstützt sowohl die 32-Bit- als auch die 64-Bit-Version. Standardmäßig erkennt das Installationsprogramm die Betriebssystemversion und installiert anschließend die entsprechende Version des Remote Loaders.

Abbildung 6-4 *Unterstützte Betriebssysteme für den Remote Loader*



Wenn Sie den Metaverzeichnis-Server als 32-Bit-Anwendung auf einem 64-Bit-Betriebssystem installiert haben, können Sie sowohl einen 32-Bit- als auch einen 64-Bit-Remote Loader auf demselben Computer installieren.

In Tabelle 6-2 werden die zertifizierten und unterstützten Betriebssysteme für den Remote Loader aufgelistet.

Tabelle 6-2 *Zertifizierte und unterstützte Betriebssysteme für den Remote Loader*

Version des Server-Betriebssystems	Zertifiziert	Unterstützt	Haftnotizen
Windows Server 2003 SP2 (32 Bit und 64 Bit)	Ja	Unterstützt auf neueren Versionen von Service Packs	Der Remote Loader läuft im 32-Bit- und im 64-Bit-Modus.
Windows Server 2008 (32- und 64-Bit)	Ja	Unterstützt auf neueren Versionen von Service Packs	Der Remote Loader läuft im 32-Bit- und im 64-Bit-Modus.
Windows Server 2008 R2 (64 Bit)	Ja	Ja	Der Remote Loader läuft nur im 64-Bit-Modus.

Version des Server-Betriebssystems	Zertifiziert	Unterstützt	Haftnotizen
Red Hat 5.7 (32 Bit und 64 Bit)	Ja	Unterstützt auf neueren Versionen von Support-Paketen	Der Remote Loader läuft im 32-Bit- und im 64-Bit-Modus. Novell empfiehlt, dass Sie vor der Installation von Identity Manager mit der automatischen Aktualisierungsfunktion des Herstellers die neuesten Betriebssystem-Patches aufspielen.
Support-Pakete für Red Hat 6.0 oder höher (32-Bit und 64-Bit)	Zertifiziert für Red Hat 6.2	Unterstützt auf neueren Versionen von Support-Paketen	Der Remote Loader läuft im 32-Bit- und im 64-Bit-Modus. Novell empfiehlt, dass Sie vor der Installation von Identity Manager mit der automatischen Aktualisierungsfunktion des Herstellers die neuesten Betriebssystem-Patches aufspielen.
SUSE Linux Enterprise Server 10 SP4 (32 Bit und 64 Bit)	Ja	Unterstützt auf neueren Versionen von Support-Paketen	Der Remote Loader läuft im 32-Bit- und im 64-Bit-Modus. Novell empfiehlt, dass Sie vor der Installation von Identity Manager mit der automatischen Aktualisierungsfunktion des Herstellers die neuesten Betriebssystem-Patches aufspielen.
SUSE Linux Enterprise Server 11 SP1 (32 Bit und 64 Bit)	Ja	Unterstützt auf neueren Versionen von Support-Paketen	Der Remote Loader läuft im 32-Bit- und im 64-Bit-Modus. Novell empfiehlt, dass Sie vor der Installation von Identity Manager mit der automatischen Aktualisierungsfunktion des Herstellers die neuesten Betriebssystem-Patches aufspielen.
SUSE Linux Enterprise Server 11 SP2 (32 Bit und 64 Bit)	Ja	Ja	Der Remote Loader läuft im 32-Bit- und im 64-Bit-Modus. Novell empfiehlt, dass Sie vor der Installation von Identity Manager mit der automatischen Aktualisierungsfunktion des Herstellers die neuesten Betriebssystem-Patches aufspielen.
OES 2 SP3 (32 Bit und 64 Bit)	Ja	Ja	Der Remote Loader läuft im 32-Bit- und im 64-Bit-Modus.
OES 11 SP1 (64-Bit)	Ja	Ja	Der Remote Loader läuft nur im 64-Bit-Modus.
Solaris 10 (64 Bit)	Ja	Ja	Der Remote Loader läuft nur im 64-Bit-Modus.

Version des Server-Betriebssystems	Zertifiziert	Unterstützt	Haftnotizen
Xen	Nein	Ja	Xen wird unterstützt, wenn die Xen Virtual Machine als Gastbetriebssystem entweder SLES 10 oder SLES 11 im paravirtualisierten Modus ausführt.
Red Hat Enterprise Linux 5 Virtualisierung (64 Bit)	Nein	Ja	Der Remote Loader läuft im 32-Bit- und im 64-Bit-Modus.
Windows Server 2008 R2 Virtualisierung mit Hyper-V (64 Bit)	Nein	Ja	Der Remote Loader läuft im 32-Bit- und im 64-Bit-Modus.

Java Remote Loader wird auf Plattformen unterstützt, auf denen der native Remote Loader nicht verfügbar ist. .NET Remote Loader wird auf Version 2 der .NET-Plattform unterstützt.

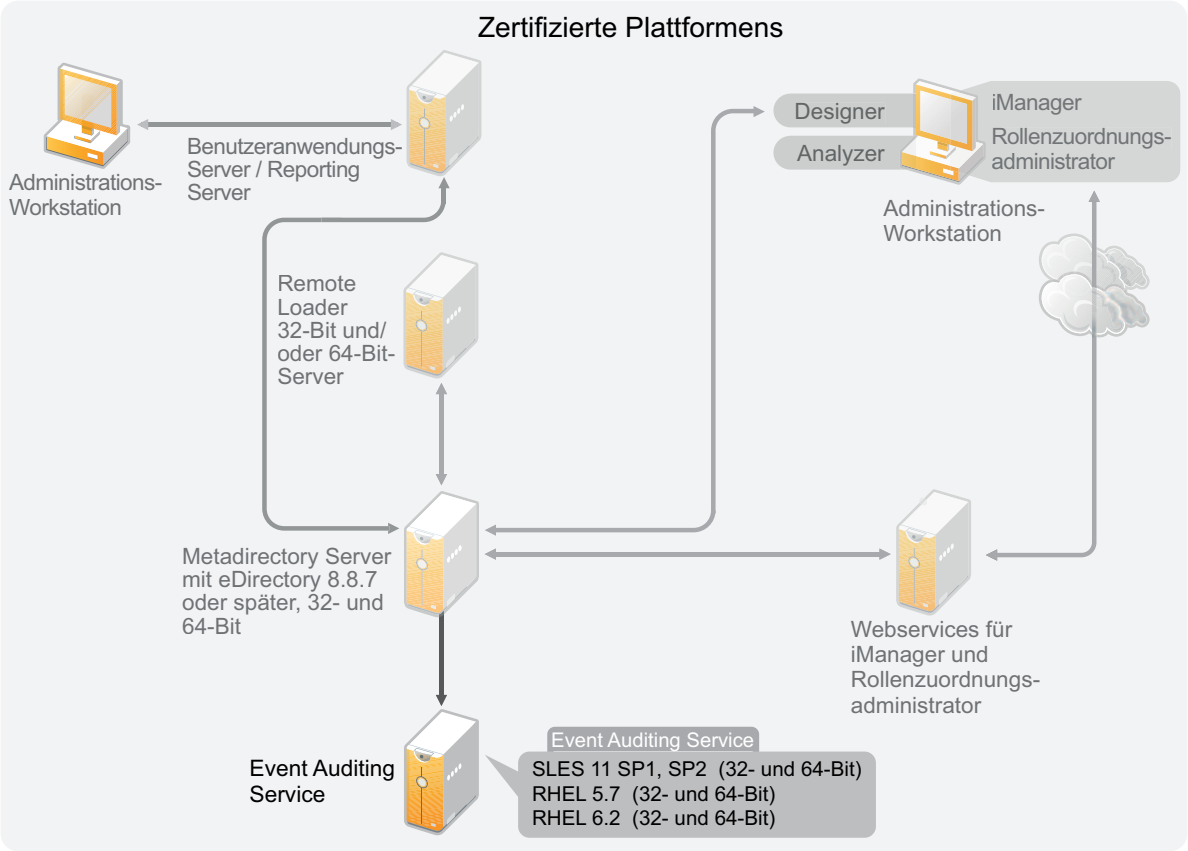
6.4 Benutzeranwendung

Informationen zu den Systemanforderungen für die Benutzeranwendung finden Sie im Abschnitt "Systemanforderungen" im *Identity Manager Roles Based Provisioning Module 4.0.2 User Application: Installation Guide* (Rollenbasiertes Bereitstellungsmodul für Identity Manager 4.0.1 Benutzeranwendung: Installationshandbuch).

6.5 Revision und Berichterstellung

Das Identitätsberichterstellungsmodul und Novell Sentinel sind zwei unterschiedliche Werkzeuge, die zum Erfassen von Revisions- und Berichtsdaten über Identity Manager verwendet werden. In Abbildung 6-5 werden die Sentinel-Versionen aufgeführt, die von Identity Manager 4.0.2 unterstützt werden.

Abbildung 6-5 *Sentinel*



Das Identitätsberichterstellungsmodul ist eine Komponente der Identity Manager Advanced Edition. Novell Sentinel ist eine optionale Komponente, die Sie zu Ihrem Identity Manager-System hinzufügen können, gehört jedoch nicht zum Lieferumfang von Identity Manager.

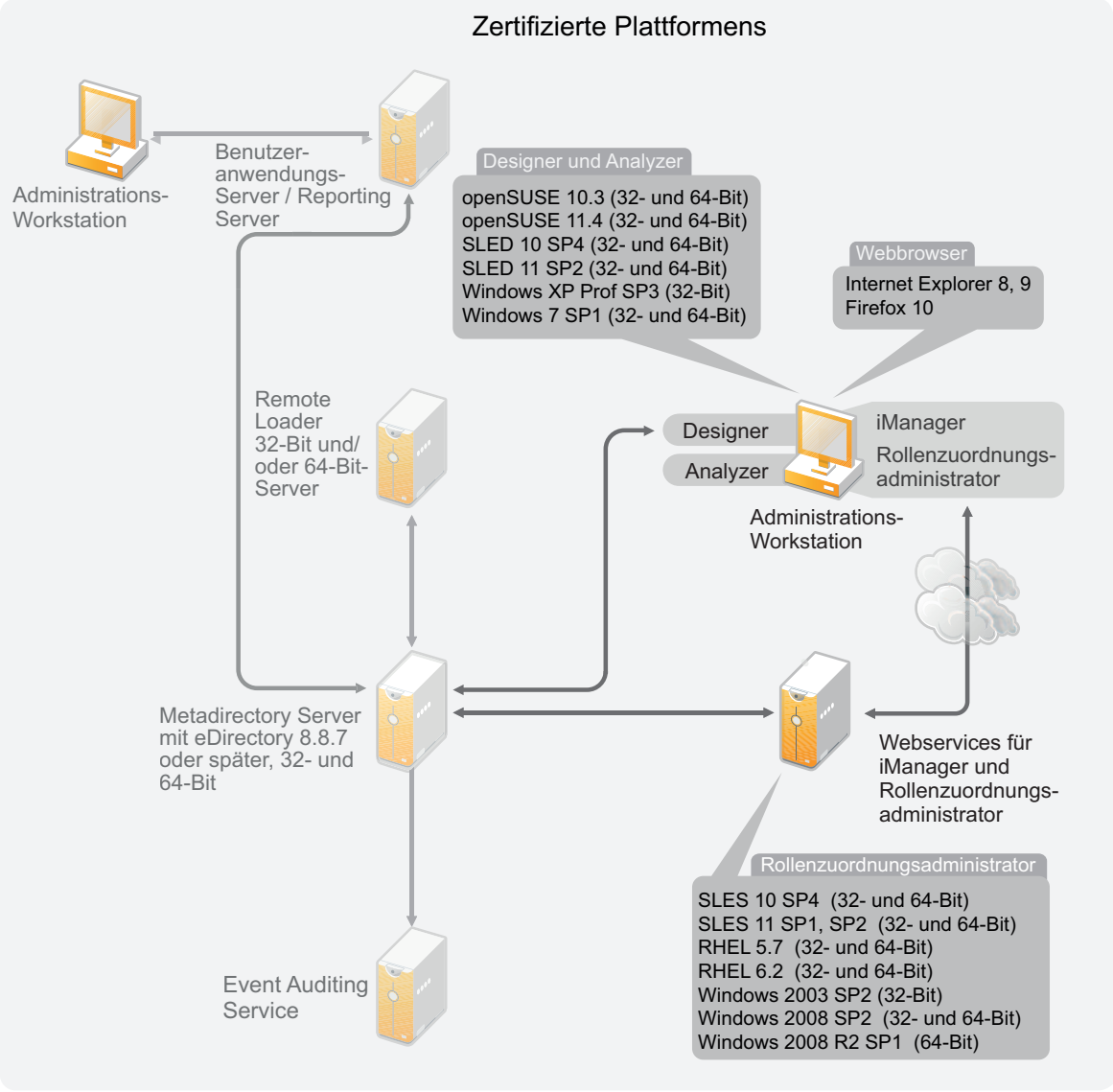
Durch die Erweiterung um die Funktionen für die Revision und die Berichterstellung können Sie die Konformitätsstandards erfüllen, die von vielen Unternehmen eingehalten werden müssen. Sie können Revisionsprotokolle für alle zu protokollierenden Ereignisse erstellen und Berichte erzeugen, um sicherzustellen, dass Sie alle für Ihr Unternehmen geltenden Revisionsstandards erfüllen.

Informationen zu Systemanforderungen und zur Konfiguration des Identitätsberichterstellungsmoduls finden Sie im Abschnitt "Systemanforderungen" im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul). Informationen zur Konfiguration von Novell Sentinel mit Identity Manager finden Sie im *Identity Manager 4.0.2 Reporting Guide for Novell Sentinel* (Identity Manager 3.6 Berichtshandbuch für Novell Sentinel). Informationen zu Systemanforderungen für Novell Sentinel finden Sie im Kapitel „Supported Platforms and Best Practices" (Unterstützte Plattformen und optimale Vorgehensweisen) im *Novell Sentinel Installation Guide* (http://www.novell.com/documentation/sentinel61/index.html) (Novell Sentinel Installationshandbuch).

6.6 Arbeitsstationen

Arbeitsstationen werden für den Zugriff auf Designer, iManager, den Rollenzuordnungsadministrator oder die Webseite für die Benutzeranwendungsverwaltung verwendet. In Abbildung 6-6 werden die unterschiedlichen Komponenten für Arbeitsstationen aufgelistet, die von Identity Manager 4.0.2 unterstützt werden.

Abbildung 6-6 *Unterstützte Komponenten für Arbeitsstationen*



Es gibt drei unterschiedliche Elemente, die Arbeitsstationen betreffen:

- Abschnitt 6.6.1, „Arbeitsstationsplattformen“, auf Seite 60
- Abschnitt 6.6.2, „Webbrowser“, auf Seite 61

6.6.1 Arbeitsstationsplattformen

Tabelle 6-3 enthält eine Liste der unterstützten Arbeitsstationsplattformen für Designer und iManager.

Informationen zu den Systemanforderungen finden Sie in der jeweiligen Komponentendokumentation.

- iManager: Siehe Abschnitt Installieren von iManager (http://www.novell.com/documentation/imanager27/imanager_install_274/data/alw39eb.html) im *Novell iManager 2.7 Installationshandbuch.*
- Designer: Siehe Abschnitt "System Requirements" (Systemanforderungen) im *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide* (Administrationshandbuch zu Designer 4.0.1 für Identity Manager 4.0.1).

Tabelle 6-3 *Unterstützte Arbeitsstationsplattformen*

Plattformen	Details
Windows 7 SP1 (32-Bit und 64-Bit)	Es werden sowohl die 32- als auch die 64-Bit-Version unterstützt.
Windows XP Professional SP3 (32-Bit)	Es wird nur die 32-Bit-Version unterstützt.
Windows 2003 SP2 (32 Bit)	Es wird nur die 32-Bit-Version unterstützt.
Windows 2008 R2 SP1 oder höher (64-Bit)	Es wird nur die 64-Bit-Version unterstützt.
Windows 2008 SP1 oder höher (32-Bit und 64-Bit)	Es werden sowohl die 32- als auch die 64-Bit-Version unterstützt.
openSUSE 10.3 (32 Bit und 64 Bit)	Wenden Sie die neuesten Patches über die automatische Aktualisierungsfunktion an.
openSUSE 11.4 (32 Bit und 64 Bit)	Wenden Sie die neuesten Patches über die automatische Aktualisierungsfunktion an.
SUSE Linux Enterprise Desktop 10 SP4 (32 Bit und 64 Bit)	Wenden Sie die neuesten Patches über die automatische Aktualisierungsfunktion an.
SUSE Linux Enterprise Desktop 11 SP2 (32-Bit und 64-Bit)	Wenden Sie die neuesten Patches über die automatische Aktualisierungsfunktion an.
SUSE Linux Enterprise Server 10 SP4 (32 Bit und 64 Bit)	Wenden Sie die neuesten Patches über die automatische Aktualisierungsfunktion an.
SUSE Linux Enterprise Server 11 SP1 oder höher (32-Bit und 64-Bit)	Wenden Sie die neuesten Patches über die automatische Aktualisierungsfunktion an.

6.6.2 Webbrowser

iManager führt alle für die Verwaltung von Identity Manager erforderlichen Plugins aus. Der Rollenzuordnungsadministrator ermöglicht Ihnen die Zuordnung von Geschäftsrollen in verschiedenen Systemen, ohne dass Sie die IT-Infrastruktur kennen müssen. Der Zugriff auf beide Anwendungen erfolgt über einen Webbrowser.

Folgende Webbrowser für iManager und den Rollenzuordnungsadministrator werden unterstützt:

- Internet Explorer 7, 8 und 9
- Mozilla Firefox 10 und höher

Eine Liste der Systemanforderungen für den Rollenzuordnungsadministrator finden Sie im Abschnitt "System Requirements" (Systemanforderungen) im *Identity Manager Role Mapping Administrator 4.0.2 Installation and Configuration Guide* (Identity Manager Role Mapping Administrator 4.0 Installations- und Konfigurationshandbuch).

6.7 Ressourcenanforderungen

Tabelle 6-4 *Identity Manager-Ressourcenanforderungen*

Identity Manager-Komponente	Mindestanforderung
Metaverzeichnis-Server	2048 MB
Remote Loader	256 MB
Treiber	200 MB
iManager-Plugins	80 MB

7 Installation von Identity Manager

Identity Manager enthält ein integriertes Installationsprogramm, das den Installationsvorgang vereinfacht und alle Komponenten gleichzeitig installiert und konfiguriert. Wenn Sie zum ersten Mal ein Identity Manager-System installieren, verwenden Sie das integrierte Installationsprogramm. Weitere Informationen finden Sie im *Identity Manager 4.0.2 Integrated Installation Guide* (Handbuch zur integrierten Installation von Identity Manager 4.0).

Wenn Sie bereits Erfahrung mit Identity Manager haben und jede Komponente einzeln installieren möchten, können Sie die für die Komponenten verfügbaren separaten Installationsprogramme verwenden.

Es ist wichtig, in der Planungsphase der Identity Manager-Implementierung Analyzer und Designer zu installieren und zu verwenden. Weitere Informationen finden Sie in Kapitel 2, „Erstellen eines Projektplans“, auf Seite 13.

Installieren Sie die Komponenten in der angegebenen Reihenfolge. Eine Erklärung der verschiedenen Komponenten finden Sie im Handbuch *Überblick über Identity Manager 4.0.2*.

- Abschnitt 7.1, „Installation von Analyzer“, auf Seite 63
- Abschnitt 7.2, „Installation von Designer“, auf Seite 64
- Abschnitt 7.3, „Installieren von eDirectory“, auf Seite 65
- Abschnitt 7.4, „Installieren von iManager“, auf Seite 66
- Abschnitt 7.5, „Installation des Metaverzeichnis-Servers“, auf Seite 66
- Abschnitt 7.6, „Installation des Remote Loaders“, auf Seite 70
- Abschnitt 7.7, „Installation der Treiberdateien“, auf Seite 76
- Abschnitt 7.8, „Installation des rollenbasierten Bereitstellungsmoduls“, auf Seite 77
- Abschnitt 7.9, „Installation eines benutzerdefinierten Treibers“, auf Seite 77
- Abschnitt 7.10, „Installation des Rollenzuordnungsadministrators“, auf Seite 77
- Abschnitt 7.11, „Installation des Identitätsberichterstellungsmoduls der Sentinel-Anwendung“, auf Seite 78
- Abschnitt 7.12, „Sprachunterstützung für die Identity Manager-Installationsprogramme“, auf Seite 78

7.1 Installation von Analyzer

Analyzer ist ein Arbeitsstation-basiertes Werkzeug, mit dem Sie Daten analysieren, bereinigen und für die Synchronisierung mit Identity Manager vorbereiten können. Sie sollten Analyzer installieren und bei der Planung der Identity Manager-Implementierung verwenden. Weitere Informationen zur Planung finden Sie in Teil I, „Planung“, auf Seite 9.

1 Stellen Sie sicher, dass das Betriebssystem Ihrer Arbeitsstation unterstützt wird.

Weitere Informationen finden Sie in Abschnitt 6.6, „Arbeitsstationen“, auf Seite 59.

2 Stellen Sie sicher, dass Sie alle erforderlichen Identity Manager-Dateien von der Download-Website von Novell heruntergeladen haben. Weitere Informationen finden Sie in Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 43.

3 Starten Sie die Installation, indem Sie das entsprechende Programm für die Plattform Ihrer Arbeitsstation ausführen.

Linux: `IDM4.0.2_Lin/products/Analyzer/install`

Führen Sie die Binärdatei aus, indem Sie `./install` eingeben.

Windows: `IDM4.0.2_Win:/products/Analyzer/install.exe`

4 Mithilfe der folgenden Informationen wird die Installation ausgeführt:

Installationsordner: Geben Sie den Ordner auf der Arbeitsstation an, in dem Analyzer installiert werden soll.

Erstellen Sie Verknüpfungen und wählen Sie eine Sprache aus: Geben Sie an, wo auf dem Desktop Verknüpfungen für Analyzer erstellt werden sollen, und wählen Sie die Sprache aus, die Sie für die Installation von Analyzer verwenden möchten.

Analyzer ist jetzt installiert. Wenn Sie Analyzer zum ersten Mal starten, werden Sie zur Aktivierung aufgefordert. Sie können Analyzer erst verwenden, wenn Sie es aktiviert haben. Weitere Informationen finden Sie in Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 81.

Informationen über eine automatische Installation von Analyzer finden Sie im Abschnitt “Automatische Installation” im *Verwaltungshandbuch zu Analyzer 4.0.2 für Identity Manager 4.0.2*.

7.2 Installation von Designer

Designer ist ein Werkzeug für Arbeitsstationen, mit dem Sie Ihre Identity Manager-Lösung entwerfen können. Sie sollten Designer installieren und bei der Planung der Identity Manager-Implementierung verwenden. Weitere Informationen zur Planung finden Sie in Teil I, „Planung“, auf Seite 9.

1 Stellen Sie sicher, dass das Betriebssystem Ihrer Arbeitsstation unterstützt wird. Installieren Sie das 32-Bit-NICI-Paket, damit Designer ordnungsgemäß funktioniert. Wenn Sie Designer auf einem 64-Bit-System installieren, stellen Sie sicher, dass die compat-Bibliothek `libgthread-2_0-0-32bit-2.17.2+2.17.3+20080708+r7171-3.1.x86_64.rpm` vor Designer installiert wird. Weitere Informationen finden Sie in Abschnitt 6.6, „Arbeitsstationen“, auf Seite 59 und im *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide* (Administrationshandbuch zu Designer 4.0.1 für Identity Manager 4.0.1).

2 Stellen Sie sicher, dass Sie alle erforderlichen Identity Manager-Dateien von der Download-Website von Novell heruntergeladen haben. Weitere Informationen finden Sie in Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 43.

3 Starten Sie die Installation, indem Sie das entsprechende Programm für die Plattform Ihrer Arbeitsstation ausführen.

Linux: `IDM4.0.2_Lin/products/Designer/install`

Führen Sie die Binärdatei aus, indem Sie `./install` eingeben.

Windows: `IDM4.0.2_Win:\products\Designer\install.exe`

4 Mithilfe der folgenden Informationen wird die Installation ausgeführt:

Installationsordner: Geben Sie den Ordner auf der Arbeitsstation an, in dem Designer installiert werden soll.

Verknüpfungen erstellen: Wählen Sie aus, ob auf Ihrem Desktop und/oder in Ihrem Desktop-Menü eine Verknüpfung erstellt werden soll.

Wenn Sie Support-Pakete für Designer wie das NICI-Paket installieren, brauchen Sie bestimmte zentrale Linux-Dienstprogramme. Die GNU-gettext-Dienstprogramme bieten einen Rahmen für internationalisierte und mehrsprachige Meldungen. Stellen Sie vor der Installation von Designer sicher, dass dieses Paket installiert wurde. Sie können YaST verwenden, um zu prüfen, welche Abhängigkeiten bestehen und welche Pakete installiert sind. Weitere Informationen finden Sie im *Verwaltungshandbuch zu Designer 4.0.2 für Identity Manager 4.0.2*.

Informationen über die automatische Installation von Designer finden Sie im Abschnitt "Automatische Installation" im *Verwaltungshandbuch zu Designer 4.0.2 für Identity Manager 4.0.2*.

7.3 Installieren von eDirectory

Stellen Sie sicher, dass Sie alle erforderlichen Identity Manager-Dateien von der Download-Website von Novell heruntergeladen haben. Weitere Informationen finden Sie in Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 43.

eDirectory 8.8.7 wird auf den Identity Manager-Datenträgern bereitgestellt. Es gibt Installationsprogramme für 32-Bit- und für 64-Bit-Plattformen. Der Speicherort des Installationsprogramms hängt von der Plattform ab:

- **Linux 32 Bit:** `IDM4.0.2_Lin/products/eDirectory/x86/setup/nds-install`
- **Linux 64 Bit:** `IDM4.0.2_Lin/products/eDirectory/x64/setup/nds-install`
- **Solaris 32 Bit:** `IDM4.0.2_Solaris/products/eDirectory/x86/setup/nds-install`
- **Solaris 64 Bit:** `IDM4.0.2_Solaris/products/eDirectory/x64/setup/nds-install`

  Führen Sie die Binärdatei aus, indem Sie `./nds-install` eingeben.
- **Windows 32 Bit:** `IDM4.0.2_Win:\products\eDirectory\x86\nt\Setup.exe`
- **Windows 64 Bit:** `IDM4.0.2_Win:\products\eDirectory\x64\windows\Setup.exe`

Die Anweisungen zur Installation von eDirectory variieren je nach verwendeter Plattform. Installationsanweisungen für Ihre Plattform finden Sie im entsprechenden Abschnitt im *Novell eDirectory 8.8 Installation Guide* (http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html) (Novell eDirectory 8.8 Installationshandbuch).

Hinweis: Für Linux und Solaris müssen Sie eDirectory nach der Installation konfigurieren, damit Sie dann den Metaverzeichnis-Server installieren können. Konfigurationsanweisungen finden Sie unter "Configuring Novell eDirectory on Linux, Solaris, or AIX Systems" (http://www.novell.com/documentation/edir88/edirin88/data/bnn8z89.html) (Konfigurieren von Novell eDirectory auf Linux-, Solaris- oder AIX-Systemen) im *Novell eDirectory 8.8 Installation Guide* (Novell eDirectory 8.8 Installationshandbuch).

Informationen über die automatische Installation von eDirectory finden Sie im *Novell eDirectory 8.8-Installationshandbuch* (http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html).

7.4 Installieren von iManager

Stellen Sie sicher, dass Sie alle erforderlichen Identity Manager-Dateien von der Download-Website von Novell heruntergeladen haben. Weitere Informationen finden Sie in Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 43.

iManager 2.7.5 wird auf den Identity Manager-Datenträgern bereitgestellt. Es stehen Installationsprogramme für Windows und Linux zur Verfügung. iManager wird unter Solaris nicht unterstützt. Der Speicherort des Installationsprogramms hängt von der Plattform ab:

- **Linux:** `IDM4.0.2_Lin/products/iManager/installs/linux/iManagerInstallLinux.bin`

  Führen Sie die Binärdatei aus, indem Sie `./iManagerInstallLinux.bin` eingeben.
- **Windows:** `IDM4.0.2_Win:\products\iManager\installs\win\iManagerInstall.exe`

Die Anweisungen zur Installation von iManager variieren je nach verwendeter Plattform. Installationsanweisungen finden Sie im entsprechenden Abschnitt im *iManager Installationshandbuch* (http://www.novell.com/documentation/imanager27/imanager_install_27/data/hk42s9ot.html).

Informationen über die automatische Installation von iManager finden Sie im Abschnitt Automatische Installation von iManager Server (http://www.novell.com/documentation/imanager27/imanager_install_274/data/bwbhk3v.html) im *iManager-Installationshandbuch* (http://www.novell.com/documentation/imanager27/imanager_install_27/data/hk42s9ot.html).

7.5 Installation des Metaverzeichnis-Servers

Auf Linux-\UNIX-Plattformen können Sie den Metaverzeichnis-Server als `root`- oder Nicht-`root`-Benutzer installieren. Bei einer Nicht-`root`-Installation verläuft der Installationsvorgang anders. Die Vorgehensweise für diese Art der Installation wird in Abschnitt 7.5.1, „Nicht-root-Installation des Metaverzeichnis-Servers“, auf Seite 68 beschrieben.

Die folgende Vorgehensweise umfasst die Benutzeroberflächeninstallation des Metaverzeichnis-Servers, der Webkomponenten und der Dienstprogramme für die von Identity Manager unterstützten Plattformen. Wenn Sie eine automatische Installation dieser Komponenten durchführen lassen möchten, lesen Sie Abschnitt 7.5.2, „Automatische Installation des Metaverzeichnis-Servers“, auf Seite 69.

1. Stellen Sie sicher, dass Ihr System den in Kapitel 6, „Systemanforderungen“, auf Seite 47 aufgeführten Systemanforderungen entspricht.
2. Stellen Sie sicher, dass Sie alle erforderlichen Identity Manager-Dateien von der Download-Website von Novell heruntergeladen haben. Weitere Informationen finden Sie in Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 43.
3. (Nur Linux\UNIX) Wenn Sie sicherstellen möchten, dass die Umgebungsvariablen für eDirectory exportiert werden, bevor die Installation unter Linux/UNIX gestartet wird, geben Sie an der Eingabeaufforderung folgenden Befehl ein:

   ```
   set | grep PATH
   ```

   Die Umgebungsvariablen legen den Pfad für die Installation von eDirectory fest. Wenn die Umgebungsvariablen festgelegt sind, wird der eDirectory-Installationspfad aufgeführt. Wenn keine Umgebungsvariablen festgelegt sind, tritt bei der Installation von Identity Manager ein Fehler auf.

   Geben Sie folgenden Befehl ein, um die Umgebungsvariablen für Ihre aktuelle Shell festzulegen:

```
. /opt/novell/eDirectory/bin/ndspath
```

Achten Sie auf das Leerzeichen zwischen dem Punkt (.) und dem Schrägstrich (/), damit der Befehl funktioniert. Weitere Informationen hierzu finden Sie unter „Using the nds-install Utility to Install eDirectory Components“ (http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#ai39feq) (Installation von eDirectory-Komponenten mithilfe des nds-install-Dienstprogramms.

4 Starten Sie die Installation, indem Sie das entsprechende Programm für Ihre Plattform ausführen.

Linux - GUI-Installation: `IDM4.0.2_Lin/products/IDM/install.bin`

Auf UNIX-Plattformen wird das Installationsprogramm standardmäßig im GUI-Modus aufgerufen. Um `idm_linux.bin` im GUI-Modus aufzurufen, müssen Sie die Option `[-i gui]` angeben.

Linux - Installation über die Befehlszeile: `IDM4.0.2_Lin/products/IDM/install.bin -i console`

Solaris - GUI-Installation: `IDM4.0.2_Solaris/products/IDM/install.bin`

Solaris - Installation über die Befehlszeile: `IDM4.0.2_Solaris/products/IDM/install.bin -i console`

Geben Sie `ein, um die Binärdateien unter Linux bzw. Solaris auszuführen./install.bin [-i {gui | console}].`

Windows: `IDM4.0.2_Win:\products\IDM\windows\setup\idm_install.exe`

5 Mithilfe der folgenden Informationen wird die Installation ausgeführt:

Komponenten auswählen: Wählen Sie den Metaverzeichnis-Server aus. Verbundene Systeme, iManager-Plug-Ins und Dienstprogramme können Sie ebenfalls auf dieser Installationsseite auswählen.

- **Novell Identity Manager - Metaverzeichnis-Server:** Für diese Option muss das Identitätsdepot auf diesem Server installiert sein. Sie installiert einen 32-Bit oder 64-Bit Identity Manager, je nachdem, welche Version von eDirectory bereits installiert ist. Sie erweitert das Schema für Identity Manager und installiert den Metaverzeichnis-Server und die Identity Manager-Treiber.
- **Novell Identity Manager - Server für verbundene Systeme (32 Bit):** Diese Option setzt nicht voraus, dass das Identitätsdepot auf diesem Server installiert ist. Wählen Sie diese Option nur, wenn Sie den Remote Loader (32 Bit) installieren. Weitere Informationen finden Sie unter Abschnitt 7.6, „Installation des Remote Loaders“, auf Seite 70.
- **Novell Identity Manager - Server für verbundene Systeme (64 Bit):** Diese Option setzt nicht voraus, dass das Identitätsdepot auf diesem Server installiert ist. Wählen Sie diese Option nur, wenn Sie den Remote Loader (64 Bit) installieren. Weitere Informationen finden Sie in Abschnitt 7.6, „Installation des Remote Loaders“, auf Seite 70.
- **Novell Identity Manager - Server für verbundene Systeme (.NET):** Mit dieser Option (nur Windows) werden der .NET Remote Loader-Service und der SharePoint-Treiber auf diesem Server installiert.
- **Novell Identity Manager-Plugins für Identity Manager:** Wählen Sie diese Option, wenn iManager auf diesem Server installiert ist. Mit dieser Option werden die iManager-Plugins für Identity Manager installiert.
- **Dienstprogramme:** Mit den Dienstprogrammen können Sie die Treiber für die verbundenen Systeme konfigurieren. Nicht für alle Treiber sind Dienstprogramme verfügbar. Wenn Sie sicher sind, dass Sie diese Funktion installieren möchten, sollten Sie sie auswählen, da sie nur wenig Festplattenspeicher benötigt.

- **Ausgewählte Komponenten anpassen:** Mit dieser Option können Sie die Komponenten anpassen, die Sie für die Installation ausgewählt haben. Bevor Sie diese Option wählen, müssen Sie zunächst die zu installierenden Komponenten auswählen.

6 Aktivieren Sie Identity Manager. Weitere Informationen finden Sie in Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 81.

7 Geben Sie einen Benutzer und das zugehörige Passwort an, der über genügend Berechtigungen zum Erweitern des Schemas in eDirectory verfügt. Geben Sie den Benutzernamen im LDAP-Format an. Beispiel: `cn=IDM-Admin,o=Firma`.

8 Erstellen und konfigurieren Sie Ihre Treiberobjekte. Diese Informationen sind in jedem Treiberhandbuch enthalten. Weitere Informationen hierzu finden Sie in der Identity Manager-Treiberdokumentation (http://www.novell.com/documentation/idm401drivers/).

9 (Optional) Die Standardinstallationsverzeichnisse sind in der Datei `/tmp/idmInstall.log` aufgeführt.

7.5.1 Nicht-root-Installation des Metaverzeichnis-Servers

Die Installation von Identity Manager als Nicht-`root`-Benutzer erhöht die Sicherheit des UNIX/Linux-Servers. Identity Manager kann nicht als Nicht-`root`-Benutzer installiert werden, falls eDirectory von einem `root`-Benutzer installiert wurde.

Bei der Nicht-`root`-Installation werden die folgenden Komponenten nicht installiert:

- **Remote Loader:** Wenn Sie den Remote Loader als Nicht-`root`-Benutzer installieren müssen, verwenden Sie den Java Remote Loader. Weitere Informationen finden Sie in Abschnitt 7.6.5, „Installation des Java Remote Loader unter UNIX oder Linux“, auf Seite 74.
- **UNIX/Linux-Kontentreiber:** Erfordert `root`-Berechtigungen.
- **Novell Sentinel-Plattformagent:** Installieren Sie den Novell Sentinel-Plattformagenten als `root`-Benutzer. Erstellen Sie die Datei `Dirxml.properties` im Verzeichnis `/etc/opt/novell/sentinelpa/conf`. `Nicht-root-Benutzer` müssen Schreibzugriff auf das Verzeichnis haben, in dem das Ereignisprotokoll generiert wird (das Standardverzeichnis ist `(/var/opt/novell/sentinelpa/data/AuditEvents.log`).

Gehen Sie wie folgt vor, um den Metaverzeichnis-Server als Nicht-`root`-Version zu installieren:

1 Stellen Sie sicher, dass Sie alle erforderlichen Identity Manager-Dateien von der Download-Website von Novell heruntergeladen haben. Weitere Informationen finden Sie in Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 43.

2 Installieren Sie eDirectory 8.8.7 oder höher als Nicht-`root`-Benutzer. Weitere Informationen hierzu finden Sie unter “Installation von eDirectory 8.8.7 durch einen Nicht-root-Benutzer” (http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#bs6a3gs).

3 Melden Sie sich mit dem Berechtigungsnachweis an, der für die Nicht-`root`-Installation von eDirectory verwendet wird.

   Identity Manager muss vom selben Benutzer installiert werden, der auch die Nicht-`root`-Installation von eDirectory ausgeführt hat. Der Benutzer, der Identity Manager installiert, muss über Schreibzugriff für die Verzeichnisse und Dateien der Nicht-`root`-Installation von eDirectory verfügen.

4 Führen Sie das Installationsprogramm für Ihre Plattform aus.

   Linux: `IDM4.0.2_Lin/products/IDM/linux/setup/idm-nonroot-install`

Solaris: `IDM4.0.2_Solaris/products/IDM/solaris/setup/idm-nonroot-install`

5 Mithilfe der folgenden Informationen wird die Installation ausgeführt:

Basisverzeichnis für die Nicht-root-Installation von eDirectory: Geben Sie das Verzeichnis an, in dem die Nicht-`root`-Version von eDirectory installiert ist. Beispiel: `/home/user/install/eDirectory`.

NDS-Schema erweitern: Wenn dies der erste Identity Manager-Server ist, der in dieser eDirectory-Instanz gespeichert wird, geben Sie zum Erweitern des Schemas `Y` ein. Wenn das Schema nicht erweitert ist, funktioniert Identity Manager nicht.

Sie werden aufgefordert, das Schema für jede eDirectory-Instanz zu erweitern, die dem Nicht-`root`-Benutzer gehören, der von der Nicht-`root`-Installation von eDirectory gehostet wird.

Wenn Sie die Schemaerweiterung auswählen, geben Sie den vollständigen eindeutigen Namen (Distinguished Name, DN) des eDirectory-Benutzers an, der über Berechtigungen zum Erweitern des Schemas verfügt. Der Benutzer kann das Schema nur erweitern, wenn er über Supervisor-Berechtigungen für die gesamte Baumstruktur verfügt. Weitere Informationen zur Erweiterung des Schemas als Nicht-`root`-Benutzer finden Sie in der Datei `schema.log`, die im `data`-Verzeichnis jeder eDirectory-Instanz gespeichert ist.

Führen Sie das Programm `/opt/novell/eDirectory/bin/idm-install-schema` aus, um das Schema nach abgeschlossener Installation auf weiteren eDirectory-Instanzen zu installieren.

Dienstprogramme: (Optional) Wenn Sie ein Identity Manager-Treiberdienstprogramm benötigen, müssen Sie die Dienstprogramme von den Datenträgern für die Identity Manager-Installation auf den Identity Manager-Server kopieren. Alle Dienstprogramme befinden sich im Verzeichnis `IDM4.0.2_`*`Plattform`*`/product/IDM/`*`Plattform`*`/setup/utilities`.

6 Aktivieren Sie Identity Manager. Weitere Informationen finden Sie in Kapitel 8, „Aktivieren von Novell Identity Manager-Produkten“, auf Seite 81.

7 Erstellen und konfigurieren Sie die Treiberobjekte. Diese Informationen sind in jedem Treiberhandbuch enthalten. Weitere Informationen hierzu finden Sie in der Identity Manager-Treiberdokumentation (http://www.novell.com/documentation/idm401drivers/).

7.5.2 Automatische Installation des Metaverzeichnis-Servers

Um eine automatische Installation von Identity Manager durchführen zu lassen, müssen Sie eine Eigenschaftendatei mit den für die Installation erforderlichen Parametern erstellen. Auf dem Identity Manager-Datenträger ist eine Beispieldatei vorhanden:

- **Linux:** `IDM4.0.2_Lin/products/IDM/linux/setup/silent.properties`
- **Solaris:** `IDM4.0.2_Solaris/products/IDM/solaris/setup/silent.properties`
- **Windows:** `IDM4.0.2_Win:\products\IDM\windows\setup\silent.properties`

Starten Sie die automatische Installation, indem Sie das entsprechende Programm für Ihre Plattform ausführen:

- **Linux:** `IDM4.0.2_Lin/products/IDM/install.bin -i silent -f <`*`Dateiname`*`>.properties`
- **Solaris:** `IDM4.0.2_Solaris/products/IDM/install.bin -i silent -f <`*`Dateiname`*`>.properties`
- **Windows:** `IDM4.0.2_Win:\products\IDM\windows\setup\idm_install.exe -i silent -f <`*`Dateiname`*`>.properties`

Erstellen Sie im Verzeichnis, in dem sich das Installationsprogramm von Identity Manager befindet, die Eigenschaftendatei `<`*`Dateiname`*`>.properties` mit den folgenden Attributen:

```
EDIR_USER_NAME=cn=admin,o=test
EDIR_USER_PASSWORD=test
METADIRECTORY_SERVER_SELECTED=true
CONNECTED_SYSTEM_SELECTED=false
X64_CONNECTED_SYSTEM_SELECTED=false
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```

Die Standardinstallationsverzeichnisse sind in der Datei `/tmp/idmInstall.log` aufgeführt.

Wenn Sie iManager installiert haben und später iManager-Plugins installieren möchten, müssen Sie den Wert `WEB_ADMIN_SELECTED` auf `true` setzen.

Wenn Sie Identity Manager auf mehreren Instanzen automatisch installieren lassen möchten, müssen Sie sicherstellen, dass die Datei *<Dateiame>*`.properties` folgende Zeilen enthält:

```
EDIR_NCP_PORT=524
EDIR_NDS_CONF=/etc/opt/novell/eDirectory/conf
EDIR_IP_ADDRESS=<xxx.xx.xx.xx>
```

Das Passwort wird in einer Datei für die automatische Installation des Metaverzeichnisses gespeichert. Sie können auch die Umgebungsvariable EDIR_USER_PASSWORD verwenden, um das Passwort bereitzustellen, statt dieses in einer Datei zu speichern. Wenn die Variable EDIR_USER_PASSWORD in der .properties-Datei nicht festgelegt ist, liest das Installationsprogramm den Wert aus der EDIR_USER_PASSWORD-Umgebungsvariable.

7.6 Installation des Remote Loaders

Der Remote Loader erweitert die Funktionalität von Identity Manager, indem er dem Treiber ermöglicht, auf das verbundene System zuzugreifen, ohne dass das Identitätsdepot und der Metaverzeichnis-Server auf demselben Server wie das verbundene System installiert sein müssen. Im Rahmen des Planungsprozesses müssen Sie sich für oder gegen die Verwendung des Remote Loader entscheiden. Weitere Informationen zum Planungsprozess finden Sie in Kapitel 3, „Technische Richtlinien“, auf Seite 25.

- Abschnitt 7.6.1, „Anforderungen“, auf Seite 71
- Abschnitt 7.6.2, „Unterstützte Treiber“, auf Seite 71
- Abschnitt 7.6.3, „Installationsvorgang“, auf Seite 72
- Abschnitt 7.6.4, „Automatische Installation des Remote Loaders“, auf Seite 74
- Abschnitt 7.6.5, „Installation des Java Remote Loader unter UNIX oder Linux“, auf Seite 74
- Abschnitt 7.6.6, „Koexistenz von 32-Bit- und 64-Bit-Remote Loader“, auf Seite 75

Wenn Sie den Remote Loader von einem Nicht-`root`-Benutzer installieren lassen möchten, verwenden Sie den Remote Loader. Der Java Remote Loader kann auch verwendet werden, wenn Sie Ihre Umgebung anpassen und den Java Remote Loader auf einer nicht unterstützten Plattform wie z. B. HP-UX installieren. Weitere Informationen finden Sie in Abschnitt 7.6.5, „Installation des Java Remote Loader unter UNIX oder Linux“, auf Seite 74.

7.6.1 Anforderungen

Der Remote Loader erfordert, dass alle verbundenen Systeme des Treibers verfügbar sind und die jeweiligen APIs zur Verfügung gestellt werden. Informationen zu den treiberspezifischen Anforderungen für das Betriebssystem und das verbundene System finden Sie in der Treiberdokumentation zu Identity Manager (http://www.novell.com/documentation/idm402drivers/).

7.6.2 Unterstützte Treiber

Nicht alle Identity Manager-Treiber werden vom Remote Loader unterstützt. Folgende Liste enthält die Treiber, die mit Remote Loader-Funktionalität ausgestattet sind.

- Active Directory
- Avaya PBX
- Banner
- Schwarzes Brett
- Datenerfassungsdienste
- Text mit Begrenzungszeichen
- Google-Apps
- GroupWise (nur für den 32-Bit-Remote Loader verfügbar)
- JDBC
- JMS
- LDAP
- Linux/UNIX-Einstellungen
- Lotus Notes
- Verwaltetes System - Gateway
- „Manuelle Aufgabe“-Services
- PeopleSoft 5.2
- Remedy ARS
- RACF
- RSA SecureID
- SalesForce.com
- SAP Business Logic
- SAP GRC (nur CMP)
- SAP HR
- SAP Portal
- SAP-Benutzerverwaltung
- Sentinel
- Integrationsmodul V2.0 für Sentinel
- Skripts
- SharePoint

- SOAP
- Streng geheim
- Auftrag

Die unten aufgeführten Treiber sind nicht mit dem Remote Loader kompatibel.

- eDirectory bidirektional
- eDirectory
- Berechtigungsservices
- Rollenservice
- Benutzeranwendung

7.6.3 Installationsvorgang

Der Remote Loader verfügt über unterschiedliche Programme für die verschiedenen Plattformen, so dass er mit dem Metaverzeichnis-Server kommunizieren kann.

- **Linux/UNIX:** `rdxml` ist eine Programmdatei, die die Kommunikation des Metaverzeichnis-Servers mit den unter Solaris- oder Linux-Umgebungen ausgeführten Identity Manager-Treibern ermöglicht.
- **Windows:** Die Remote Loader-Konsole verwendet `rlconsole.exe` für die Kopplung mit `dirxml_remote.exe`. Dies ist eine Programmdatei, die die Kommunikation des Metaverzeichnis-Servers mit den unter Windows ausgeführten Identity Manager-Treibern ermöglicht.

So installieren Sie den Remote Loader:

1. Stellen Sie sicher, dass Ihr System den in Kapitel 6, „Systemanforderungen“, auf Seite 47 aufgeführten Systemanforderungen entspricht.
2. Stellen Sie sicher, dass Sie alle erforderlichen Identity Manager-Dateien von der Download-Website von Novell heruntergeladen haben. Weitere Informationen finden Sie in Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 43.
3. Starten Sie die Installation, indem Sie das entsprechende Programm für Ihre Plattform ausführen.

   Linux - GUI-Installation: `IDM4.0.2_Lin/products/IDM/install.bin`

   Linux - Installation über die Befehlszeile: `IDM4.0.2_Lin/products/IDM/install.bin -i console`

   Solaris - GUI-Installation: `IDM4.0.2_Solaris/products/IDM/install.bin`

   Solaris - Installation über die Befehlszeile: `IDM4.0.2_Solaris/products/IDM/install.bin -i console`

   Windows: `IDM4.0.2_Win:\products\IDM\windows\setup\idm_install.exe`

   Geben Sie `ein, um die Binärdateien unter Linux bzw. Solaris auszuführen./install.bin [-i {gui | console}].`
4. Mithilfe der folgenden Informationen wird die Installation ausgeführt:

Komponenten auswählen: Wählen Sie den Server und die Dienstprogramme des verbundenen Systems aus, um den Remote Loader zu installieren.

- **Novell Identity Manager - Metaverzeichnis-Server:** Wählen Sie diese Option nur, wenn Sie den Metaverzeichnis-Server installieren. Diese Option setzt voraus, dass das Identitätsdepot auf diesem Server installiert ist. Weitere Informationen finden Sie in Abschnitt 7.5, „Installation des Metaverzeichnis-Servers“, auf Seite 66.
- **Novell Identity Manager - Server für verbundene Systeme (32 Bit):** Diese Option setzt nicht voraus, dass das Identitätsdepot auf diesem Server installiert ist. Sie installiert die 32-Bit-Version des Remote Loader-Service auf Ihrem Anwendungsserver.
- **Novell Identity Manager - Server für verbundene Systeme (64 Bit):** Diese Option setzt nicht voraus, dass das Identitätsdepot auf diesem Server installiert ist. Sie installiert die 64-Bit-Version des Remote Loader-Service auf Ihrem Anwendungsserver.
- **Novell Identity Manager - Server für verbundene Systeme (.NET):** Mit dieser Option (nur Windows) werden der .NET Remote Loader-Service und der SharePoint-Treiber auf diesem Server installiert.
- **Novell Identity Manager-Plugins für Identity Manager:** Wählen Sie diese Option, wenn iManager auf diesem Server installiert ist. Mit dieser Option werden die iManager-Plugins für Identity Manager installiert.
- **Benutzerdefiniert:** Wählen Sie diese Option, wenn Sie die installierten Funktionen anpassen möchten. Sie ermöglicht Ihnen die Auswahl der unten aufgeführten Optionen. Bevor Sie diese Option wählen, sollten Sie die zu installierenden Komponenten auswählen:
  - **Remote Loader-Service (32 Bit):** Der Service, der mit dem Metaverzeichnis-Server kommuniziert.
  - **Remote Loader-Service (64 Bit):** Der Service, der mit dem Metaverzeichnis-Server kommuniziert.
  - **Treiber:** Wählen Sie aus, welche Treiberdateien installiert werden sollen. Es wird empfohlen, alle Treiberdateien zu installieren. So müssen Sie die Installation nicht erneut ausführen, wenn Sie eine weitere Remote Loader-Instanz hinzufügen.
  - **Novell Identity Manager - Server für verbundene Systeme (.NET):** (Nur Windows) Installiert den .NET Remote Loader-Service und den SharePoint-Treiber.

  Wenn Sie keine der oben aufgeführten Optionen auswählen, kann die benutzerdefinierte Installation nicht fortgesetzt werden.

(Nur Windows) Installationsverzeichnis des Servers für verbundene Systeme: Geben Sie das Verzeichnis an, in dem der Server des verbundenen Systems installiert wird.

(Nur Windows) Installationsort für den .Net Remote Loader: Geben Sie das Verzeichnis an, in dem der .NET Remote Loader installiert ist.

(Nur Windows) Installationsverzeichnis für Dienstprogramme: Geben Sie das Verzeichnis an, in dem die Dienstprogramme installiert sind.

5 Erstellen und konfigurieren Sie Ihre Treiberobjekte so, dass sie den Remote Loader verwenden. Diese Informationen sind in jedem Treiberhandbuch enthalten. Weitere Informationen hierzu finden Sie in der Identity Manager-Treiberdokumentation (http://www.novell.com/documentation/idm402drivers/).

6 Erstellen Sie eine Konfigurationsdatei, damit Remote Loader zusammen mit dem verbundenen System verwendet werden kann. Weitere Informationen finden Sie unter “Configuring the Remote Loader for Linux/UNIX by Creating a Configuration File” (Konfiguration des Remote Loader für Linux/UNIX durch Erstellung einer Konfigurationsdatei) im *Identity Manager 4.0.2 Remote Loader Guide* (Handbuch zum Identity Manager 4.0 Remote Loader).

7.6.4 Automatische Installation des Remote Loaders

Um eine automatische Installation des Remote Loader durchführen zu lassen, müssen Sie eine Eigenschaftendatei mit den für die Installation erforderlichen Parametern erstellen. Auf dem Identity Manager-Datenträger ist eine Beispieldatei vorhanden:

- **Linux:** `IDM4.0.2_Lin/products/IDM/linux/setup/silent.properties`
- **Solaris:** `IDM4.0.2_Solaris/products/IDM/solaris/setup/silent.properties`
- **Windows:** `IDM4.0.2_Win:\products\IDM\windows\setup\silent.properties`

Starten Sie die automatische Installation, indem Sie das entsprechende Programm für Ihre Plattform ausführen:

- **Linux:** `IDM4.0.2_Lin/products/IDM/install.bin -i silent -f <Dateiname>.properties`
- **Solaris:** `IDM4.0.2_Solaris/products/IDM/install.bin -i silent -f <Dateiname>.properties`
- **Windows:** `IDM4.0.2_Win:\products\IDM\windows\setup\idm_install.exe -i silent -f <Dateiname>.properties`

Erstellen Sie im Verzeichnis, in dem sich das Installationsprogramm von Identity Manager befindet, die Eigenschaftendatei `<Dateiname>.properties` mit den folgenden Attributen:

```
METADIRECTORY_SERVER_SELECTED=false
CONNECTED_SYSTEM_SELECTED=true
X64_CONNECTED_SYSTEM_SELECTED=true
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```

Die Standardinstallationsverzeichnisse sind in der Datei `/tmp/idmInstall.log` aufgeführt.

Wenn Sie iManager installiert haben und später iManager-Plugins installieren möchten, müssen Sie den Wert `WEB_ADMIN_SELECTED` auf `true` setzen.

7.6.5 Installation des Java Remote Loader unter UNIX oder Linux

`dirxml_jremote` ist ein reiner Java-Remote-Loader. Er wird zum Datenaustausch zwischen dem auf einem Server aktiven Metaverzeichnis-Server und den Identity Manager-Treibern verwendet, die an einem anderen Standort ausgeführt werden, auf dem `rdxml` nicht ausgeführt wird. Er sollte auf jedem System mit einer kompatiblen JRE (ab 1.5.0) und Java Sockets ausgeführt werden können. Er wird von allen Linux-/UNIX-Plattformen unterstützt, die von Identity Manager unterstützt werden.

1. Stellen Sie sicher, dass Java 1.5.x JDK/JRE auf dem Host-System verfügbar ist.
2. Stellen Sie sicher, dass Sie alle erforderlichen Identity Manager-Dateien von der Download-Website von Novell heruntergeladen haben. Weitere Informationen finden Sie in Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 43.
3. Suchen Sie die Installationsdateien für den Java Remote Loader auf dem Identity Manager-Datenträger:

   Linux: `IDM4.0.2_Lin/products/IDM/java_remoteloader`

   Solaris: `IDM4.0.2_Solaris/products/IDM/java_remoteloader`
4. Kopieren Sie die Datei `dirxml_jremote_dev.tar.gz` an den gewünschten Speicherort auf dem Remote-Server.

5 Kopieren Sie die Datei `dirxml_jremote.tar.gz` oder `dirxml_jremote_mvs.tar` an den gewünschten Speicherort auf dem Remote-Server.

   Beispiel: `/usr/idm`

   Wenn Sie Informationen zu mvs benötigen, dekomprimieren Sie die Datei `dirxml_jremote_mvs.tar` und öffnen Sie das Dokument `usage.html`.

6 Entpacken und extrahieren Sie die Dateien `dirxml_jremote.tar.gz` und `dirxml_jremote_dev.tar.gz`.

   Beispiel: `gunzip dirxml_jremote.tar.gz` bzw. `tar -xvf dirxml_jremote_dev.tar`

7 Kopieren Sie die `.jar`-Dateien des Anwendungsschnittstellenmoduls in das Unterverzeichnis `lib`, das beim Extrahieren der `dirxml_jremote.tar`-Datei erstellt wurde.

   Da die tar-Datei nicht die `.jar`-Dateien enthält, müssen Sie diese `.jar`-Dateien manuell vom Metaverzeichnis-Server in das `lib`-Verzeichnis kopieren. Das `lib`-Verzeichnis befindet sich in dem von Ihnen zuvor dekomprimierten Verzeichnis.

   Das Standardinstallationsverzeichnis für `.jar`-Dateien auf dem Metaverzeichnis-Server ist `/opt/novell/eDirectory/lib/dirxml/classes`.

8 Passen Sie das `dirxml_jremote`-Skript an, indem Sie einen der folgenden Schritte ausführen:

   - Stellen Sie sicher, dass die Java-Programmdatei durch die Umgebungsvariable PATH erreichbar ist, indem Sie die Umgebungsvariable RDXML_PATH festlegen. Legen Sie die Umgebungsvariable mithilfe der folgenden Befehle fest:

     1. `set RDXML_PATH=path`
     2. `export RDXML_PATH`

   - Bearbeiten Sie das `dirxml_jremote`-Skript und fügen Sie den Pfad der Java-Programmdatei am Anfang der Skriptzeile ein, die Java ausführt.

9 Konfigurieren Sie die Beispieldatei `config8000.txt` am Speicherort `/opt/novell/dirxml/doc` zur Verwendung mit Ihrem Anwendungsschnittstellenmodul. Weitere Informationen finden Sie unter "Configuring the Remote Loader for Linux/UNIX by Creating a Configuration File" (Konfiguration des Remote Loader für Linux/UNIX durch Erstellung einer Konfigurationsdatei) im *Identity Manager 4.0.2 Remote Loader Guide* (Handbuch zum Identity Manager 4.0 Remote Loader).

7.6.6 Koexistenz von 32-Bit- und 64-Bit-Remote Loader

Identity Manager 4.0.2 lässt zu, dass die 32-Bit- und die 64-Bit-Version von Remote Loader auf einem 64-Bit-Betriebssystem gleichzeitig installiert sind. Wenn Sie eine 32-Bit-Version von Remote Loader auf einem 64-Bit-Betriebssystem aufrüsten, wird der 32-Bit-Remote Loader aufgerüstet und gleichzeitig wird der 64-Bit-Remote Loader installiert. Sie können den 32-Bit- und den 64-Bit-Remote Loader auf demselben Computer installieren.

Wenn Sie wählen, sowohl einen 32-Bit- als auch einen 64-Bit-Remote Loader auf demselben Computer zu installieren, werden die Audit-Ereignisse nur mit dem 64-Bit-Remote Loader generiert. Wenn zuerst ein 64-Bit-Remote Loader und dann ein 32-Bit-Remote Loader installiert wird, werden die Ereignisse im 32-Bit-lcache protokolliert.

7.7 Installation der Treiberdateien

Sie können die Treiberdateien ohne den Metaverzeichnis-Server oder den Remote Loader installieren. Die Treiberdateien bestehen aus Treiberschnittstellenmodulen und den Treiber-Dienstprogrammen.

So installieren Sie die Treiberdateien:

1. Stellen Sie sicher, dass Sie alle erforderlichen Identity Manager-Dateien von der Download-Website von Novell heruntergeladen haben. Weitere Informationen finden Sie in Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 43.
2. Starten Sie die Installation, indem Sie das entsprechende Programm für Ihre Plattform ausführen.

   Linux - GUI-Installation: `IDM4.0.2_Lin/products/IDM/install.bin [-i gui]`

   Linux - Installation über die Befehlszeile: `IDM4.0.2_Lin/products/IDM/install.bin -i console`

   Solaris - GUI-Installation: `IDM4.0.2_Solaris/products/IDM/install.bin [-i gui]`

   Solaris - Installation über die Befehlszeile: `IDM4.0.2_Solaris/products/IDM/install.bin -i console`

   Geben Sie `ein, um die Binärdateien unter Linux bzw. Solaris auszuführen./install.bin [-i {gui | console}].`

   Windows: `IDM4.0.2_Win:\products\IDM\windows\setup\idm_install.exe`
3. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf *Weiter*.
4. Wählen Sie auf der Seite „Komponenten auswählen“ folgende Optionen aus:

   Novell Identity Manager - Metaverzeichnis-Server: Sie können diese Option oder die Option *Server für verbundene Systeme* auswählen. Sie müssen nicht beide Optionen auswählen.

   Die Treiberdateien sind in dieser Option enthalten.

   Novell Identity Manager - Server für verbundene Systeme: Sie können diese Option oder die Option *Metaverzeichnis-Server* auswählen. Sie müssen nicht beide Optionen auswählen.

   Die Treiberdateien sind in dieser Option enthalten.

   Novell-Dienstprogramme Wählen Sie diese Option, um Dienstprogramme zu installieren, die bei der Konfiguration einiger Treiber helfen.

   Ausgewählte Komponenten anpassen: Ermöglicht es Ihnen, nur die Treiberdateien auszuwählen, ohne den Metaverzeichnis-Server oder den Remote Loader zu installieren.
5. Klicken Sie auf *Weiter*.
6. Heben Sie die Auswahl der Optionen *Metaverzeichnis-Engine* und *Remote Loader Service* auf, falls sie in Schritt 4 auf Seite 76 ausgewählt sind.
7. Stellen Sie sicher, dass die Option *Treiber* unter der Option *Metaverzeichnis-Server* oder *Server für verbundene Systeme* ausgewählt ist.

   Sie können die Option *Treiber* erweitern und nur die Treiber auswählen, die Sie installieren möchten. Standardmäßig werden alle Treiber ausgewählt.
8. Klicken Sie auf *Weiter*.
9. Geben Sie auf der Seite *Authentifizierung* einen Benutzer und das zugehörige Passwort an, der über genügend Berechtigungen zum Erweitern des Schemas in eDirectory verfügt. Geben Sie den Benutzernamen im LDAP-Format an. Beispiel: `cn=IDM-Admin,o=Firma`.

10 Klicken Sie auf *Weiter*.

11 Überprüfen Sie die Zusammenfassung der Installation und klicken Sie anschließend auf *Installieren*.

12 Überprüfen Sie die Meldung „Installation abgeschlossen“ und klicken Sie auf *Fertig*.

Die Treiberdateien werden nun mit dem Remote Loader oder dem Metaverzeichnis-Server installiert.

7.8 Installation des rollenbasierten Bereitstellungsmoduls

Informationen zur Installation des rollenbasierten Bereitstellungsmoduls finden Sie im *Identity Manager Roles Based Provisioning Module 4.0.2 User Application: Installation Guide* (Rollenbasiertes Bereitstellungsmodul für Identity Manager 4.0 Benutzeranwendung: Installationshandbuch).

7.9 Installation eines benutzerdefinierten Treibers

Sie können einen benutzerdefinierten Treiber erstellen, der in Ihrer Umgebung verwendet werden soll. Weitere Informationen zur Erstellung oder Installation eines benutzerdefinierten Treibers finden Sie im Novell Developer Kit (http://developer.novell.com/wiki/index.php/Dirxml).

7.10 Installation des Rollenzuordnungsadministrators

Der Rollenzuordnungsadministrator ist ein Webservice, der die Autorisierungen und Berechtigungen ermittelt, die innerhalb Ihres Haupt-IT-Systems erteilt werden können.

Hinweis: Der Rollenzuordnungsadministrator ist in der Standard Edition nicht verfügbar.

So installieren Sie den Rollenzuordnungsadministrator:

1 Stellen Sie sicher, dass Sie alle erforderlichen Identity Manager-Dateien von der Download-Website von Novell heruntergeladen haben. Weitere Informationen finden Sie in Kapitel 5, „Bezugsquellen für Identity Manager“, auf Seite 43.

2 Suchen Sie die Installationsdatei für den Rollenzuordnungsadministrator auf dem Identity Manager-Datenträger, der sich hier befindet:

Linux: `IDM4.0.2_Lin/products/RMA/IDMRMAP.jar`

Windows: `IDM4.0.2_Win:\products\RMA\IDMRMAP.jar`

3 Wechseln Sie über eine Befehlszeile in das Installationsverzeichnis des Rollenzuordnungsadministrators und geben Sie Folgendes ein: `java -jar IDMRMAP.jar`.

Hinweis: Aus Sicherheitsgründen sollten Sie den Rollenzuordnungsadministrator auf Linux-Plattformen als Nicht-`root`-Benutzer installieren.

---

4 Geben Sie `Ja` ein, um die Lizenzvereinbarung zu akzeptieren.

5 Geben Sie das Installationsverzeichnis für den Rollenzuordnungsadministrator an. Der Standardpfad ist das aktuelle Verzeichnis.

6 Geben Sie den Teil der URL an, der den Namen des Rollenzuordnungsadministrator repräsentiert. Der Standardwert ist IDMRMAP.

7 Geben Sie den HTTP-Port an. Der Standardwert ist 8081.

8 Geben Sie ein Passwort für den Konfigurationsadministrator an.

Der Rollenzuordnungsadministrator ist nun installiert. Die Anwendung wird nach Abschluss der Installation nicht automatisch gestartet. Verwenden Sie folgende Skripte im Installationsverzeichnis, um die Anwendung zu stoppen und zu starten.

- **Linux:** Das Startskript ist `start.sh`, das Stoppskript `stop.sh`.
- **Windows:** Das Startskript ist `start.bat`, das Stoppskript `stop.bat`.

Wenn der Rollenzuordnungsadministrator installiert und gestartet wurde, müssen Sie ihn konfigurieren. Konfigurationsinformationen finden Sie unter "Configuring the Application" (Konfigurieren der Anwendung) im *Identity Manager Role Mapping Administrator 4.0.2 Installation and Configuration Guide* (Installations- und Konfigurationshandbuch zum Identity Manager-Rollenzuordnungsadministrator 2.0).

7.11 Installation des Identitätsberichterstellungsmoduls der Sentinel-Anwendung

Das Identitätsberichterstellungsmodul und Sentinel sind optionale Komponenten für die Identity Manager-Lösung. Durch die Erweiterung um die Funktionen für die Revision und die Berichterstellung können Sie die Konformitätsstandards erfüllen, die von vielen Unternehmen eingehalten werden müssen. Sie können Revisionsprotokolle für alle zu protokollierenden Ereignisse erstellen sowie Berichte generieren, um sicherzustellen, dass Sie alle für Ihr Unternehmen geltenden Revisionsstandards erfüllen.

Informationen zur Installation und Konfiguration des Identitätsberichterstellungsmoduls finden Sie im *Handbuch zum Identitätsberichterstellungsmodul*. Informationen zur Konfiguration von Novell Sentinel mit Identity Manager finden Sie im *Identity Manager 3.6 Berichterstellungshandbuch für Novell Sentinel*. Informationen zu den Systemanforderungen für Sentinel finden Sie im *Novell Sentinel Installation Guide* (http://www.novell.com/documentation/sentinel6/index.html) (Novell Sentinel Installationshandbuch).

7.12 Sprachunterstützung für die Identity Manager-Installationsprogramme

Die einzelnen Identity Manager-Installationsprogramme unterstützen verschiedene Sprachen.

- **Metaverzeichnis-Server:** Traditionelles Chinesisch, vereinfachtes Chinesisch, Deutsch, Französisch und Japanisch.
- **Integriertes Installationsprogramm:** Traditionelles Chinesisch, vereinfachtes Chinesisch, Deutsch, Französisch und Japanisch.
- **Rollenbasiertes Bereitstellungsmodul:** Traditionelles Chinesisch, vereinfachtes Chinesisch, Dänisch, Deutsch, Französisch, Italienisch, Japanisch, Niederländisch, brasilianisches Portugiesisch, Russisch, Schwedisch und Spanisch.
- **Identitätsberichterstellungsmodul:** Traditionelles Chinesisch, vereinfachtes Chinesisch, Dänisch, Deutsch, Französisch, Niederländisch, Italienisch, Japanisch, brasilianisches Portugiesisch, Russisch, Schwedisch und Spanisch.

- **Designer:** Traditionelles Chinesisch, vereinfachtes Chinesisch, Französisch, Deutsch, Italienisch, Japanisch, Niederländisch, brasilianisches Portugiesisch und Spanisch.

  Hinweis: Installieren Sie unter Linux die gettext-Dienstprogramme. Die GNU-gettext-Dienstprogramme bieten einen Rahmen für internationalisierte und mehrsprachige Meldungen.

- **Analyzer:** Englisch.
- **Rollenzuordnungsadministrator:** Englisch.

Beim Starten eines Identity Manager-Installationsprogramms gelten die folgenden Bedingungen:

- Wenn das Betriebssystem in einer Sprache ausgeführt wird, die das Identity Manager-Installationsprogramm unterstützt, wählt die Sprachauswahl im Identity Manager-Installationsprogramm standardmäßig diese Sprache aus.
- Wenn das Betriebssystem in einer Sprache ausgeführt wird, die das Identity Manager-Installationsprogramm nicht unterstützt, wählt die Sprachauswahl im Identity Manager-Installationsprogramm standardmäßig Englisch aus.
- Wenn das Betriebssystem in einer lateinischen Sprache ausgeführt wird, stehen in der Sprachauswahl auch alle anderen lateinischen Sprachen zur Verfügung.
- Wenn das Betriebssystem in einer asiatischen Sprache oder in Russisch ausgeführt wird, stehen in der Sprachauswahl nur die Sprache des Betriebssystems und Englisch zur Verfügung.

Die Identity Manager-Installationsprogramme erkennen das Gebietsschema eines Systems und entscheiden, welche Sprache unterstützt wird. Ändern Sie zur Installation einer neuen Sprache auf Ihrem System das Gebietsschema unter Windows anhand der Option *Regionale Einstellungen*. Legen Sie unter Linux/Solaris die LANG-Variable im Profil oder über die Befehlszeile fest.

Identity Manager unterstützt die folgenden lateinischen Sprachen:

- Dänisch
- Niederländisch
- Englisch
- Französisch
- Deutsch
- Italienisch
- Portugiesisch (Brasilien)
- Spanisch
- Schwedisch

Weitere von Identity Manager unterstützte Sprachen:

- **Asiatische Sprachen** Japanisch, traditionelles Chinesisch und vereinfachtes Chinesisch.
- **Kyrillische Sprachen:** Russisch.

7.12.1 Überlegungen zu Sprachen, die nicht von den Installationsprogrammen unterstützt werden

Obwohl Designer in neun Sprachen lokalisiert ist, sind die Identity Manager-Treiber nur in fünf Sprachen lokalisiert. Wenn die Treibersprache nicht unterstützt wird, erfolgt die Treiberkonfiguration standardmäßig in Englisch.

Alle iManager-Plug-Ins für Identity Manager sind in fünf Sprachen übersetzt. Vier iManager-Plug-Ins sind ins Spanische, Russische, Italienische und Portugiesische übersetzt. Auf lokalisierten Systemen sind die lokalisierten Plug-Ins übersetzt, alle anderen Plug-Ins werden in Englisch ausgeführt. Auf dänischen, niederländischen und schwedischen Systemen werden alle Plug-Ins in Englisch ausgeführt.

8 Aktivieren von Novell Identity Manager-Produkten

Im Folgenden wird erläutert, wie die Aktivierung von Produkten erfolgt, die auf Novell Identity Manager basieren. Identity Manager, die Integrationsmodule und das Bereitstellungsmodul müssen innerhalb von 90 Tagen nach der Installation aktiviert werden, anderenfalls werden sie außer Betrieb gesetzt. Sie können Identity Manager-Produkte zu einem beliebigen Zeitpunkt während oder nach Ablauf der 90 Tage aktivieren.

Führen Sie zur Aktivierung von Identity Manager und den Treibern folgende Schritte aus:

- Abschnitt 8.1, „Erwerb einer Produktlizenz für Identity Manager“, auf Seite 81
- Abschnitt 8.2, „Installation einer Produktaktivierungsberechtigung“, auf Seite 82
- Abschnitt 8.3, „Anzeigen der Produktaktivierungen für Identity Manager und Identity Manager-Treiber“, auf Seite 83
- Abschnitt 8.4, „Aktivieren von Identity Manager-Treibern“, auf Seite 83
- Abschnitt 8.5, „Aktivieren von Analyzer“, auf Seite 84
- Abschnitt 8.6, „Aktivieren von Designer und dem Rollenzuordnungsadministrator“, auf Seite 84

8.1 Erwerb einer Produktlizenz für Identity Manager

Informationen zum Kauf einer Identity Manager-Produktlizenz für die Aktivierung des Produkts finden Sie auf der Novell Identity Manager-Bestellwebseite (http://www.novell.com/products/identitymanager/howtobuy.html)

Wenn Sie eine Produktlizenz erworben haben, wird Ihnen von Novell die Kunden-ID per Email zugesendet. Die Email enthält außerdem die URL der Website, auf der Sie eine Produktaktivierungsberechtigung erhalten. Wenn Sie Ihre Kundennummer vergessen oder keine Nummer erhalten haben, rufen Sie in den USA das Novell Activation Center unter 1-800-418-8373 an. In allen anderen Ländern rufen Sie bitte +1-801-861-8373 an. Sie können auch online mit uns chatten (http://support.novell.com/chat/activation).

8.2 Installation einer Produktaktivierungsberechtigung

Die Produktaktivierungsberechtigung sollte über iManager installiert werden.

1. Nach dem Erwerb einer Lizenz erhalten Sie von Novell eine Email mit Ihrer Kunden-ID. Die Email enthält außerdem unter „Auftragsdetails“ einen Link zur Website, auf der Sie einen Berechtigungsnachweis erhalten. Rufen Sie die Website auf, indem Sie auf den Link klicken.
2. Klicken Sie auf den Link zum Herunterladen der Lizenz und führen Sie einen der folgenden Schritte aus:
   - Speichern Sie die Datei mit der Produktaktivierungsberechtigung.

     oder
   - Öffnen Sie die Datei mit der Produktaktivierungsberechtigung und kopieren Sie ihren Inhalt in die Zwischenablage.

     Achten Sie darauf, dass in der Kopie keine zusätzlichen Zeilen oder Leerzeichen eingefügt werden. Markieren Sie den zu kopierenden Text vom ersten Gedankenstrich (-) der Berechtigung (----BEGINN DER PRODUKTAKTIVIERUNGSBERECHTIGUNG) bis zum letzten Gedankenstrich (-) der Berechtigung (ENDE DER PRODUKTAKTIVIERUNGSBERECHTIGUNG-----).

     Warnung: Wenn die Aktivierung der Standard Edition auf ein vorhandenes, nicht aktiviertes Advanced Edition-System angewendet wird, werden der Identity Manager-Metaverzeichnis-Server und die Treiber angehalten.
3. Öffnen Sie iManager.
4. Wählen Sie *Identity Manager* > *Identity Manager-Überblick*.
5. Klicken Sie auf , um in der Baumstruktur nach einem Treibersatz zu suchen und diesen auszuwählen.
6. Klicken Sie auf der Seite „Identity Manager-Überblick“ auf den Treibersatz, der den zu aktivierenden Treiber enthält.
7. Klicken Sie auf der Seite „Treibersatz-Überblick“ auf *Aktivierung* > *Installation*.
8. Wählen Sie den Treibersatz aus, in dem Sie eine Identity Manager-Komponente aktivieren möchten, und klicken Sie anschließend auf *Weiter*.
9. Führen Sie einen der folgenden Vorgänge aus:
   - Geben Sie an, wo Sie den Identity Manager-Berechtigungsnachweis gespeichert haben, und klicken Sie auf *Weiter*.

     oder
   - Kopieren Sie den Inhalt der Datei in den Textbereich und klicken Sie auf *Weiter*.
10. Klicken Sie auf *Fertig stellen*.

Hinweis: Sie müssen jeden Treibersatz aktivieren, in dem ein Treiber vorhanden ist, den Sie verwenden möchten. Sie können mit dem Berechtigungsnachweis jeden Baum aktivieren.

8.3 Anzeigen der Produktaktivierungen für Identity Manager und Identity Manager-Treiber

Für jeden Treibersatz werden die Produktaktivierungsberechtigungen angezeigt, die Sie für die Metaverzeichnis-Server- und Identity Manager-Treiber installiert haben:

1. Öffnen Sie iManager.
2. Klicken Sie auf *Identity Manager* > *Identity Manager-Überblick*.
3. Klicken Sie auf das , um einen Treibersatz in der Baumstruktur zu suchen, und klicken Sie anschließend auf das , um die Suche durchzuführen.
4. Klicken Sie auf der Seite „Identity Manager-Überblick“ auf den Treibersatz, dessen Aktivierungsinformationen Sie anzeigen möchten.
5. Klicken Sie auf der Seite „Treibersatz-Überblick“ auf *Aktivierung* > *Informationen*.

   Sie können den Text des Berechtigungsnachweises anzeigen oder bei einer Fehlermeldung einen Berechtigungsnachweis entfernen.

Hinweis: Nach der Installation einer gültigen Produktaktivierungsberechtigung wird neben dem Treibernamen möglicherweise noch immer „Aktivierung erforderlich“ angezeigt. Starten Sie in diesem Fall den Treiber neu. Die Meldung sollte dann nicht mehr angezeigt werden.

8.4 Aktivieren von Identity Manager-Treibern

Mit dem Kauf von Identity Manager haben Sie auch Aktivierungen für Service-Treiber und verschiedene allgemeine Treiber erworben.

- **Service-Treiber:** Folgende Service-Treiber werden aktiviert, wenn Sie den Metaverzeichnis-Server aktivieren:
  - Datenerfassungsdienst
  - Berechtigungsservices
  - ID-Provider
  - Loopback-Service
  - Verwaltetes System - Gateway
  - 'Manuelle Aufgabe'-Service
  - Null-Service
  - Rollenservice
  - Benutzeranwendung
  - Auftrag
- **Allgemeine Treiber:** Folgende allgemeine Treiber werden aktiviert, wenn Sie den Metaverzeichnis-Server aktivieren:
  - Active Directory
  - ADAM
  - eDirectory
  - GroupWise

- LDAP
- Lotus Notes

Aktivierungen für alle anderen Identity Manager-Treiber müssen separat erworben werden. Die Aktivierungen für die Treiber sind als Identity Manager-Integrationsmodule erhältlich. Ein Identity Manager-Integrationsmodul kann einen oder mehrere Treiber enthalten. Sie erhalten für jedes erworbene Identity Manager-Integrationsmodul eine Produktaktivierungsberechtigung.

Sie müssen die Schritte in Abschnitt 8.2, „Installation einer Produktaktivierungsberechtigung“, auf Seite 82 für jedes Identity Manager-Integrationsmodul ausführen, um die Treiber zu aktivieren.

8.5 Aktivieren von Analyzer

Wenn Sie Analyzer zum ersten Mal starten, werden Sie zur Aktivierung aufgefordert. Wenn Sie die Aktivierung nicht vornehmen, können Sie Analyzer nicht verwenden. Weitere Informationen finden Sie unter “Activating Analyzer” (Aktivieren von Analyzer) im *Analyzer 4.0.2 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.1 für Identity Manager).

8.6 Aktivieren von Designer und dem Rollenzuordnungsadministrator

Designer und der Rollenzuordnungsadministrator erfordern keine weiteren Aktivierungen zusätzlich zur Aktivierung des Metaverzeichnis-Servers oder der Treiber.

9 Fehlerbehebung in Identity Manager

Bei der Installation von Identity Manager sollten Sie Folgendes beachten:

- „Lotus Notes-Treiberproblem beim Installieren von Identity Manager“, auf Seite 85
- „Die Identity Manager-Installation kann auf der 32-Bit-Plattform von Windows 2008 SP2 gelegentlich fehlschlagen.“, auf Seite 86
- „Die Remotedesktopinstallation von Identity Manager funktioniert möglicherweise nicht“, auf Seite 89
- „Die Hilfeseite zur Remote Loader-Konsole wird unter Windows Server 2008 Core nicht angezeigt“, auf Seite 89
- „Probleme beim Aufrufen eines Installationsprogramms im GUI-Modus“, auf Seite 89
- „Wenn zwei Ereignisse beim Syntax-Datenstromattribut auftreten, geht die erste Attributsänderung verloren“, auf Seite 89
- „Ändern des Passworts in der Benutzeranwendung“, auf Seite 90
- „lcache-Problem während der Identity Manager-Aufrüstung“, auf Seite 90
- „Beim Aufrüsten von Identity Manager ist das richtige Administratorkonto erforderlich, damit keine Herausforderungsantworten verloren gehen“, auf Seite 90
- „Unter SLES 11 bleibt das Identity Manager-Installationsprogramm bei der Aufrüstung von Identity Manager mit mehreren Instanzen von eDirectory hängen“, auf Seite 91
- „Wenn Sie auf virtuellen Computern eDirectory starten, wird die Identity Manager-Engine aufgrund eines Fehlers von JNI_CreateJavaVM möglicherweise nicht geladen“, auf Seite 91

Lotus Notes-Treiberproblem beim Installieren von Identity Manager

Ursprung: Wenn Sie als Nicht-`root`-Benutzer Identity Manager 4.0.2 unter Solaris 10 installieren, wird möglicherweise der folgende Fehler für den Lotus Notes-Treiber angezeigt:

```
ln: cannot create /usr/lib/locale/ja/wnn//ndsrep: File exists
ln: cannot create
cp: cannot create /usr/lib/locale/ja/wnn//libnotesdrvjni.so.1.0.0:
Permission
denied
ln: cannot create /usr/lib/locale/ja/wnn//libnotesdrvjni.so.1:
File exists
ln: cannot create /usr/lib/locale/ja/wnn//libnotesdrvjni.so: File
exists
```

Aktion: Erstellen Sie manuell die symbolischen Links. Weitere Informationen zum Prüfen und Neuerstellen von symbolischen Links finden Sie unter “Troubleshooting Installation Problems” (Beheben von Installationsproblemen) im *Identity Manager 4.0.2 Driver for Lotus Notes Implementation Guide* (Handbuch für die Implementierung des Identity Manager 3.6.1-Treibers für Lotus Notes).

Die Identity Manager-Installation kann auf der 32-Bit-Plattform von Windows 2008 SP2 gelegentlich fehlschlagen.

Ursprung: Das Framework-Installationsprogramm zeigt folgenden Fehler an:

```
Java Platform SE binary has stopped working.
```

Aktion: So können Sie das Problem umgehen:

1. Führen Sie das Identity Manager-Installationsprogramm mit der Option *-DCLUSTER_INSTALL="true"* aus. Hierdurch werden nur die Identity Manager-Dateien und nicht das eDirectory-Schema oder andere Dateien installiert.

   ```
   <install_drive>:\windows\setup\idm_install.exe -
   DCLUSTER_INSTALL="true"
   ```

2. Erweitern Sie das Identity Manager-Schema durch iManager, indem Sie den *Assistenten zum Importieren, Konvertieren, Exportieren* unter *eDirectory-Wartung* verwenden.

3. Erstellen Sie Standardobjekte mithilfe der LDIF-Datei.

   - LDIF-Datei mit Standardpasswortrichtlinie

     ```
     dn: cn=Password Policies,cn=Security
     objectClass: nspmPasswordPolicyContainer
     objectClass: Top
     cn: Password Policies
     ACL: 1#subtree#[Public]#[Entry Rights]
     ACL: 3#subtree#[Public]#[All Attributes Rights]

     dn: cn=Sample Challenge Set,cn=Password
     Policies,cn=Security
     objectClass: nsimChallengeSet
     objectClass: Top
     cn: Sample Challenge Set

     dn: cn=Sample Password Policy,cn=Password
     Policies,cn=Security
     objectClass: nspmPasswordPolicy
     objectClass: Top
     cn: Sample Password Policy
     ```

   - LDIF-Datei mit Richtlinie für die Standard-Benachrichtigungserfassung

     ```
     dn: cn=Default Notification Collection,cn=Security
     objectClass: notfTemplateCollection
     objectClass: Top
     cn: Default Notification Collection
     ACL: 1#subtree#[Public]#[Entry Rights]
     ACL: 3#subtree#[Public]#[All Attributes Rights]

     dn: cn=Password Expiration Notification,cn=Default
     Notification Collection,cn=Security
     notfMergeTemplateSubject: Password Expiration Notification
     notfMergeTemplateData::
     PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3ZlbGwuY29tL2Rpc
     nhtbC93b3JrZmxvdy9mb3JtIj4gDQo8Zm9ybTp0b2tlbi1kZXNjcmlwdG
     lvbnM+IA0KPGZvcm06dG9rZW4tZGVzY3JpcHRpb24gZGVzY3JpcHRpb24
     9IkZ1bGwgbmFtZSBieSB3aGljaCB0byBhZGRyZXNzIHVzZXIiIGl0ZW0t
     bmFtZT0iVXNlckZ1bGxOYW1lIi8+IA0KPGZvcm06dG9rZW4tZGVzY3Jpc
     HRpb24gZGVzY3JpcHRpb249Ik51bWJlciBvZiBkYXlzIHVudGlsIHBhc3
     N3b3JkIGV4cGlyZXMiIGl0ZW0tbmFtZT0iRXhwRGF5cyIvPiANCjwvZm9
     ybTp0b2tlbi1kZXNjcmlwdGlvbnM+IA0KPGhlYWQ+IA0KPHRpdGxlPlBh
     ```

```
c3N3b3JkIEV4cGlyYXRpb24gTm90aWZpY2F0aW9uPC90aXRsZT4gDQo8c
3R5bGU+IA0KPCEtLSBib2R5IHsgZm9udC1mYW1pbHk6IFRyZWJ1Y2hldC
BNUyB9IC0tPiANCjwvc3R5bGU+IA0KPC9oZWFkPiANCjxib2R5IEJHQ09
MT1I9IiNGRkZGRkYiPiANCjxwPkRlYXIgJFVzZXJGdWxsTmFtZSQsPC9w
PiANCjxwPlRoaXMgbWVzc2FnZSBpcyB0byBpbmZvcm0geW91IHRoYXQge
W91ciBwYXNzd29yZCB3aWxsIGV4cGlyZSBpbjwvcD4gDQo8YnIvPiANCi
AgJEV4cERheXMkIGRheXM8YnIvPiANCjxici8+IA0KPHA+UGxlYXNlIHB
sYW4gdG8gY2hhbmdlIHlvdXIgcGFzc3dvcmQgYmVmb3JlIGl0IGV4cGly
ZXMuPC9wPiANCjxwPiAtIEF1dG9tYXRlZCBTZWN1cml0eSAtIDwvcD4gD
Qo8cD4gDQo8aW1nIEFMVD0iUG93ZXJlZCBieSBOb3ZlbGwiIFNSQz0iY2
lkOnBvd2VyZWRfYnlfbm92ZWxsLmdpZiIgaGVpZ2h0PSIyOSIgd2lkdGg
9IjgwIi8+IA0KPC9wPiANCjwvYm9keT4gDQo8L2h0bWw+IA0K
objectClass: notfMergeTemplate
objectClass: Top
cn: Password Expiration Notification

dn: cn=Password Reset Fail,cn=Default Notification
Collection,cn=Security
notfMergeTemplateSubject: Notice of Password Reset Failure
notfMergeTemplateData::
PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3ZlbGwuY29tL2Rpc
nhtbC93b3JrZmxvdy9mb3JtIj4NCiAgPGZvcm06dG9rZW4tZGVzY3JpcH
Rpb25zPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9uIGl0ZW0tbmF
tZT0iVXNlckZ1bGxOYW1lIiBkZXNjcmlwdGlvbj0iVGhlIHVzZXIncyBm
dWxsIG5hbWUiLz4NCiAgICA8Zm9ybTp0b2tlbi1kZXNjcmlwdGlvbiBpd
GVtLW5hbWU9IlVzZXJHaXZlbk5hbWUiIGRlc2NyaXB0aW9uPSJUaGUgdX
NlcidzIGdpdmVuIG5hbWdDT0xPUj0iI0ZGRkZGRiI+DQogIDxwPkRlYXI
gJFVzZXJGdWxsTmFtZSQsPC9wPg0KICA8cD5UaGlzIGlzIGEgbm90aWNl
IHRoYXQgeW91ciBwYXNzd29yZCBjb3VsZCBub3QgYmUgcmVzZXQgaW4gd
GhlICRDb25uZWN0ZWRTeXN0ZW1OYW1lJCBzeXN0ZW0uLiAgVGhlIHJlYX
NvbiBmb3IgZmFpbHVyZSBpcyBpbmRpY2F0ZWQgYmVsb3c6PC9wPg0KICA
8cD5SZWFzb246ICRGYWlsdXJlUmVhc29uJDwvcD4NCiAgPHA+SWYgeW91
IGhhdmUgYW55IGZ1cnRoZXIgcXVlc3Rpb25zLA0KICAgICBwbGVhc2UgY
29udGFjdCB0aGUgaGVscCBkZXNrIGF0ICgwMTIpIDM0NS02Nzg5IG9yIG
VtYWlsDQogICAgIGF0IDxhIGhyZWY9Im1haWx0bzpoZWxwLmRlc2tAbXl
jb21wYW55LmNvbSI+DQogICAgIGhlbHAuZGVza0BteWNvbXBhbnkuY29t
IDwvYT48L3A+DQogIDxwPiAtIEF1dG9tYXRlZCBTZWN1cml0eTwvcD4NC
iAgPHA+PGltZyBTUkM9ImNpZDpwb3dlcmVkX2J5X25vdmVsbC5naWYiIE
FMVD0iUG93ZXJlZCBieSBOb3ZlbGwiIHdpZHRoPSI4MCIgaGVpZ2h0PSI
yOSIvPjwvcD4NCjwvYm9keT4NCjwvaHRtbD4NCg==
objectClass: notfMergeTemplate
objectClass: Top
cn: Password Reset Fail

dn: cn=Password Set Fail,cn=Default Notification
Collection,cn=Security
notfMergeTemplateSubject: Notice of Password Set Failure
notfMergeTemplateData::
PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3ZlbGwuY29tL2Rpc
nhtbC93b3JrZmxvdy9mb3JtIj4NCiAgPGZvcm06dG9rZW4tZGVzY3JpcH
Rpb25zPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9uIGl0ZW0tbmF
tZT0iVXNlckZ1bGxOYW1lIiBkZXNjcmlwdGlvbj0iVGhlIHVzZXIncyBm
dWxsIG5hbWUiLz4NCiAgICA8Zm9ybTp0b2tlbi1kZXNjcmlwdGlvbiBpd
GVtLW5hbWU9IlVzZXJHaXZlbk5hbWUiIGRlc2NyaXB0aW9uPSJUaGUgdX
NlcidzIGdpdmVuIG5hbWU4NCiAgICA8Zm9ybTp0b2tlbi1kZXNjcml
wdGlvbiBpdGVtLW5hbWU9IlVzZXJMYXN0TmFtZSIgZGVzY3JpcHRpb249
IlRoZSB1c2VyJ3MgbGFzdCBuYW1lIi8+DQogICAgPGZvcm06dG9rZW4tZ
GVzY3JpcHRpb24gaXRlbS1uYW1lPSJDb25uZWN0ZWRTeXN0ZW1OYW1lIi
BkZXNjcmlwdGlvbj0iVGhlIGV4dGVybmFsIGFwcGxpY2F0b24gbmFtZSI
vPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9uIGl0ZW0tbmFtZT0i
RmFpbHVyZVJlYXNvbiIgZGVzY3JpcHRpb249IlRoZSBmYWlsdXJlIHJlY
XNvbiIvPg0KICA8L2Zvcm06dG9rZW4tZGVzY3JpcHRpb25zPg0KPGhlYW
Q+DQogIDx0aXRsZT5Ob3RpY2UgdGhhdCB5b3VyIHBhc3N3b3JkIGNvdWx
kIG5vdCBlZSBzZXQgaW4gdGhlICRDb25uZWN0ZWRTeXN0ZW1OYW1lJCBz
eXN0ZW0uLiAgVGhlIHJlYXNvbiBmb3IgZmFpbHVyZSBpcyBpbmRpY2F0
ZWQgYmVsb3c6PC9wPg0KICA8cD5SZWFzb246ICRGYWlsdXJlUmVhc29uJ
DwvcD4NCiAgPHA+SWYgeW91IGhhdmUgYW55IGZ1cnRoZXIgcXVlc3Rpb2
5zLA0KICAgICBwbGVhc2UgY29udGFjdCB0aGUgaGVscCBkZXNrIGF0ICg
wMTIpIDM0NS02Nzg5IG9yIGVtYWlsDQogICAgIGF0IDxhIGhyZWY9Im1h
aWx0bzpoZWxwLmRlc2tAbXljb21wYW55LmNvbSI+DQogICAgIGhlbHAuZ
GVza0BteWNvbXBhbnkuY29tIDwvYT48L3A+DQogIDxwPiAtIEF1dG9tYX
RlZCBTZWN1cml0eTwvcD4NCiAgPHA+PGltZyBTUkM9ImNpZDpwb3dlcmV
kX2J5X25vdmVsbC5naWYiIHdpZHRoPSI4MCIgaGVpZ2h0PSIyOSIvPjwv
cD4NCjwvYm9keT4NCjwvaHRtbD4NCg==
```

```
lsdXJlUmVhc29uJDwvcD4NCiAgPHA+SWYgeW91IGhhdmUgYW55IGZ1cnR
oZXIgcXVlc3Rpb25zLA0KICAgICBwbGVhc2UgY29udGFjdCB0aGUgaGVs
cCBkZXNrIGF0ICgwMTIpIDM0NS02Nzg5IG9yIGVtYWlsDQogICAgIGF0I
DxhIGhyZWY9Im1haWx0bzpoZWxwLmRlc2tAbXljb21wYW55LmNvbSI+DQ
ogICAgIGhlbHAuZGVza0BteWNvbXBhbnkuY29tIDwvYT48L3A+DQogIDx
wPiAtIEF1dG9tYXRlZCBTZWN1cml0eTwvcD4NCiAgPHA+PGltZyBTUkM9
ImNpZDpwb3dlcmVkX2J5X25vdmVsbC5naWYiIEFMVD0iUG93ZXJlZCBie
SBOb3ZlbGwiIHdpZHRoPSI4MCIgaGVpZ2h0PSIyOSIvPjwvcD4NCjwvYm
9keT4NCjwvaHRtbD4NCg==
objectClass: notfMergeTemplate
objectClass: Top
cn: Password Set Fail

dn: cn=Password Sync Fail,cn=Default Notification
Collection,cn=Security
notfMergeTemplateSubject: Notice of Password
Synchronization Failure
notfMergeTemplateData::
PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3ZlbGwuY29tL2Rpc
nhtbC93b3JrZmxvdy9mb3JtIj4NCiAgPGZvcm06dG9rZW4tZGVzY3JpcH
Rpb25zPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9uIGl0ZW0tbmF
tZT0iVXNlckZ1bGxOYW1lIiBkZXNjcmlwdGlvbj0iVGhlIHVzZXIncyBm
dWxsIG5hbWUiLz4NCiAgICA8Zm9ybTp0b2tlbi1kZXNjcmlwdGlvbiBpd
GVtLW5hbWU9IlVzZXJHaXZlbk5hbWUiIGRlc2NyaXB0aW9uPSJUaGUgdX
NlcidzIGdpdmVuIG5hbWUiLz4NCiAgICA8Zm9ybTp0b2tlbi1kZXNjcml
wdGlvbiBpdGVtLW5hbWU9IlVzZXJMYXN0TmFtZSIgZGVzY3JpcHRpb249
IlRoZSB1c2VyJ3MgbGFzdCBuYW1lIi8+DQogICAgPGZvcm06dG9rZW4tZ
GVzY3JpcHRpb24gaXRlbS1uYW1lPSJDb25uZWN0ZWRTeXN0ZW1OYW1lIi
BkZXNjcmlwdGlvbj0iVGhlIGV4dGVybmFsIGFwcGxpY2F0b24gbmFtZSI
vPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9uIGl0ZW0tbmFtZT0i
RmFpbHVyZVJlYXNvbiIgZGVzY3JpcHRpb249IlRoZSBmYWlsdXJlIHJlY
XNvbiIvPg0KICA8L2Zvcm06dG9rZW4tZGVzY3JpcHRpb25zPg0KPGhlYW
Q+DQogIDx0aXRsZT5Ob3RpY2Ugb2YgUGFzc3dvcmQgU3luY2hyb25pemF
0aW9uIEZhaWx1cmU8L3RpdGxlPg0KICA8c3R5bGU+IDwhLS0gYm9keSB7
IGZvbnQtZmFtaWx5OiBUcmVidWNoZXQgTVMgfSAtLT4gPC9zdHlsZT4NC
jwvaGVhZD4NCjxib2R5IEJHQ09MT1I9IiNGRkZGRkYiPg0KICA8cD5EZW
FyICRVc2VyRnVsbE5hbWUkLDwvcD4NCiAgPHA+VGhpcyBpcyBhIG5vdGl
jZSB0aGF0IHlvdXIgcGFzc3dvcmQgZnJvbSB0aGUgJENvbm5lY3RlZFN5
c3RlbU5hbWUkIHdhcyB1bmFibGUgdG8gc3luY2hyb25pemUgdG8gb3RoZ
XIgY29ubmVjdGVkIHN5c3RlbXMuICBUaGUgcmVhc29uIGZvciBmYWlsdX
JlIGlzIGluZGljYXRlZCBiZWxvdzo8L3A+DQogIDxwPlJlYXNvbjogJEZ
haWx1cmVSZWFzb24kPC9wPg0KICA8cD5JZiB5b3UgaGF2ZSBhbnkgZnVy
dGhlciBxdWVzdGlvbnMsIHBsZWFzZSBjb250YWN0IHRoZSBoZWxwIGRlc
2sgYXQgKDAxMikNCiAgICAgMzQ1LTY3ODkgb3IgZW1haWwgYXQgPGEgaH
JlZj0ibWFpbHRvOmhlbHAuZGVza0BteWNvbXBhbnkuY29tIj4NCiAgICA
gaGVscC5kZXNrQG15Y29tcGFueS5jb20gPC9hPjwvcD4NCiAgPHA+IC0g
QXV0b21hdGVkIFNlY3VyaXR5PC9wPg0KICA8cD48IC0tPg0KICA8cD48aW1nIFNQz0iY2lkO
nBvd2VyZWRfYnlfbm92ZWxsLmdpZiIgQUxUPSJQb3dlcmVkIGJ5IE5vdm
VsbCIgd2lkdGg9IjgwIiBoZWlnaHQ9IjI5Ii8+PC9wPg0KPC9ib2R5Pg0
KPC9odG1sPg0K
objectClass: notfMergeTemplate
objectClass: Top
cn: Password Sync Fail
```

4 Installieren Sie die NMAS-Methoden.

5 Wählen Sie nach der Installation der NMAS-Plugins auf iManager *NMAS > NMAS Login > Methods > New.* Suchen und installieren Sie die Konfigurationsdateien der gewünschten NMAS-Methoden.

Hinweis: Stellen Sie sicher, dass Sie in der Protokolldatei nachsehen, bevor Sie die Ausweichlösung anwenden. Wenn z. B. das Schema des rollenbasierten Bereitstellungsmoduls bereits erweitert ist, müssen Sie es während der Installation des Treibers für das rollenbasierte Bereitstellungsmodul nicht erweitern.

Die Remotedesktopinstallation von Identity Manager funktioniert möglicherweise nicht

Mögliche Ursache: Wenn Sie Identity Manager von einem Remote Desktop aus installieren, schlägt die Installation möglicherweise fehl und es wird eine Fehlermeldung angezeigt. Da die Remotedesktopverbindung im Vergleich zur tatsächlichen/physischen Adresse verzögert ist, kann der Installationsvorgang die lokalen Verweise nicht erfassen, was zum Fehlschlagen der Installation führt.

Aktion: Sie können das Problem umgehen, indem Sie Identity Manager auf einer tatsächlichen/physischen Verbindung des Servers oder unter Verwendung einer VNC-Verbindung installieren

Die Hilfeseite zur Remote Loader-Konsole wird unter Windows Server 2008 Core nicht angezeigt

Mögliche Ursache: Wenn Sie unter Windows Server 2008 Core in der Remote Loader-Konsole auf *Hilfe* klicken, wird die entsprechende Hilfeseite nicht angezeigt.

Aktion: Sie können dieses Problem umgehen, indem Sie einen Browser, z. B. Internet Explorer, auf Ihrem Computer installieren und in der Remote Loader-Konsole auf *Hilfe* klicken.

Probleme beim Aufrufen eines Installationsprogramms im GUI-Modus

Mögliche Ursache: Eine Fehlermeldung wird angezeigt, wenn das integrierte Installationsprogramm im GUI-Modus aufgerufen wird, falls die erforderlichen RPMs nicht im System vorhanden sind. Das integrierte Installationsprogramm wechselt automatisch in den Konsolenmodus, der nicht unterstützt wird.

Aktion: Installieren Sie die erforderlichen RPMs, bevor Sie das Identity Manager-Installationsprogramm aufrufen.

In der Identity Manager 4.0.2 Readme (http://www.novell.com/documentation/idm402/readme/data/idm402_readme.html#bwnkb9a) finden Sie eine Liste der RPMs, die für eine erfolgreiche Installation und Konfiguration von Identity Manager erforderlich sind.

Wenn zwei Ereignisse beim Syntax-Datenstromattribut auftreten, geht die erste Attributsänderung verloren

Ursprung: Die Identity Manager 4.0.2 Engine speichert die Attribute STREAM und OCTET_STRING nicht im Cache. Wenn ein Ereignis mit dem verbundenen System synchronisiert wird, liest die Engine diese Attribute aus dem Identitätsdepot und aktualisiert das verbundene System. Wenn diese Attribute geändert werden, bevor die Engine sie aus dem Identitätsdepot liest, werden die geänderten Werte im verbundenen System aktualisiert, die Zwischenänderung geht jedoch möglicherweise verloren.

Aktion: Wenn das Attribut häufig geändert wird, verwenden Sie eine andere passende Syntax anstelle von SYN_STREAM.

Wenn beispielsweise ein XML-Objekt im Attribut STREAM gespeichert ist, verwenden Sie die XMLData-Syntax anstelle von SYN_STREAM.

Ändern des Passworts in der Benutzeranwendung

Mögliche Ursache: Die Benutzeranwendung geht davon aus, dass der eDirectory-Server so eingestellt ist, dass bei der Anmeldung die Umgebungsvariable NMASLOGIN_FIRST verwendet werden muss. Das Identity Manager-Installationsprogramm erledigt dies automatisch, indem es das Skript pre_ndsd_start für Linux bzw. den Registrierungsschlüssel `HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Environment` für Windows ändert.

Wenn Sie eine Standardinstallation von eDirectory durchführen, für einen vorhandenen Benutzer eine Passwortrichtlinie anwenden, sich anschließend als dieser Benutzer anmelden und einen Vorgang des Typs „Passwort vergessen“ durchführen, wird nach Beantworten der Sicherheitsabfragen möglicherweise folgende Meldung angezeigt: Universelles Passwort ist nicht festgelegt.

Aktion: So können Sie das Problem umgehen,

1. **Linux/UNIX:** Fügen Sie die folgenden zwei Zeilen in das Skript pre_ndsd_start ein. Das Skript befindet sich unter `/opt/novell/eDirectory/sbin` (zuvor `/etc/init.d`):

   ```
   NDSD_TRY_NMASLOGIN_FIRST=true

   export NDSD_TRY_NMASLOGIN_FIRST
   ```

   Windows: Klicken Sie mit der rechten Maustaste auf *Eigener Computer* und wählen Sie *Eigenschaften* aus. Klicken Sie auf der Registerkarte *Erweitert* auf *Umgebungsvariablen*. Fügen Sie unter *Systemvariablen* die Variable hinzu und legen Sie den Wert auf *Wahr* fest. Führen Sie diesen Schritt auf allen Servern aus, die NMAS-Anmeldungen per LDAP handhaben.
2. Führen Sie einen Neustart von eDirectory durch, damit die Änderungen wirksam werden.

lcache-Problem während der Identity Manager-Aufrüstung

Ursprung: Nach dem Aufrüsten von Identity Manager protokolliert der Plattformagent Ereignisse möglicherweise nicht wie gewünscht. Dieses Problem tritt auf, weil der Plattformagent während der Identity Manager-Aufrüstung unter Linux nicht aufgerüstet wird. Unter Solaris wird der Plattformagent auf die neueste Version aufgerüstet, der neue Plattformagent hat jedoch andere Standardports, sodass ein Neustart von lcache erforderlich ist.

Aktion: Sie müssen lcache manuell anhalten, bevor Sie die Aufrüstung starten.

Beim Aufrüsten von Identity Manager ist das richtige Administratorkonto erforderlich, damit keine Herausforderungsantworten verloren gehen

Ursprung: Beim Aufrüsten von einer früheren Version von Identity Manager auf der Windows-Plattform sollten Sie dasselbe Administratorkonto verwenden, das auch für die Installation von eDirectory verwendet wurde.

Erklärung: Wenn beispielsweise die Installation von eDirectory mit einem Domänenadministratorkonto vorgenommen wurde, verwenden Sie dasselbe Domänenadministratorkonto zum Installieren von Identity Manager. Verwenden Sie kein lokales Administratorkonto.

Aktion: Wenn Sie nicht das gleiche Administratorkonto verwenden, ist kein Zugriff auf die Benutzerantworten auf die Herausforderungsfragen mehr möglich. Dies hängt damit zusammen, dass der Baumschlüssel während der Installation neu erstellt wird (wegen der unterschiedlichen Administratorkonten) und der neue Baumschlüssel keinen richtigen Zugriff auf die gespeicherten Antworten ermöglicht. Benutzer werden bei der Anmeldung aufgefordert, neue Herausforderungsantworten einzugeben.

Unter SLES 11 bleibt das Identity Manager-Installationsprogramm bei der Aufrüstung von Identity Manager mit mehreren Instanzen von eDirectory hängen

Aktion: Vor der Aufrüstung des Metaverzeichnisses auf einem Server mit mehreren eDirectory-Instanzen müssen Sie sich vergewissern, dass sich im Verzeichnis `/etc/opt/novell/eDirectory/conf/.edir/` nur eine Datei mit einer eDirectory-Instanz befindet. Sie müssen die einzelnen eDirectory-Instanzen separat aufrüsten, um die Editionsinformationen für jede Instanz einzufügen und das Schema für jede Instanz zu erweitern. In Artikel TID 7008633 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7008633&sliceId=2&docTypeID=DT_TID_1_1&dialogID=238490556&stateId=0%200%20238492510) finden Sie weitere Informationen zur Aufrüstung des Metaverzeichnisses auf einem Server mit mehreren eDirectory-Instanzen.

Wenn Sie auf virtuellen Computern eDirectory starten, wird die Identity Manager-Engine aufgrund eines Fehlers von JNI_CreateJavaVM möglicherweise nicht geladen

Ursprung: Dieses Problem tritt nur auf virtuellen Maschinen auf.

Aktion: So können Sie das Problem umgehen:

1. Starten Sie eDirectory neu.
2. Verringern Sie die Mindestgröße des JVM-Heaps, falls dieser Fehler wiederholt auftritt.
3. Starten Sie eDirectory neu.

10 Neue Funktionen

Identity Manager 4.0.2 enthält verschiedene neue Funktionen und Verbesserungen:

- Abschnitt 10.1, „Neuerungen in Identity Manager 4.0.2“, auf Seite 93

Eine Liste der Funktionen und Verbesserungen in Identity Manager 4.0 und 4.0.1 finden Sie in den folgenden Abschnitten:

- Abschnitt 10.2, „Neuerungen in Identity Manager 4.0.1“, auf Seite 97
- Abschnitt 10.3, „Neuerungen in Identity Manager 4.0“, auf Seite 98

10.1 Neuerungen in Identity Manager 4.0.2

- Abschnitt 10.1.1, „Neue Treiber“, auf Seite 93
- Abschnitt 10.1.2, „Funktionen für die Passwortverwaltung“, auf Seite 94
- Abschnitt 10.1.3, „Funktionen für den Rollenzuordnungsadministrator“, auf Seite 94
- Abschnitt 10.1.4, „Funktionen des rollenbasierten Provisioning-Moduls“, auf Seite 95
- Abschnitt 10.1.5, „Funktionen für das Identitätsberichterstellungsmodul“, auf Seite 95
- Abschnitt 10.1.6, „Designer-Funktionen“, auf Seite 96
- Abschnitt 10.1.7, „Analyzer-Funktionen“, auf Seite 97

10.1.1 Neue Treiber

Die folgenden neuen Treiber sind in Identity Manager 4.0.2 enthalten:

- **Bidirektionaler eDirectory-Treiber:** Der bidirektionale eDirectory-Treiber von Identity Manager synchronisiert Daten zwischen dem Identitätsdepot und eDirectory. Weitere Informationen hierzu finden Sie im *Identity Manager 4.0.2 Driver for Bidirectional eDirectory Implementation Guide* (Implementierungshandbuch für den Identity Manager 4.0.2-Treiber für bidirektionales eDirectory).
- **Sentinel Identity Tracking Driver Implementation Guide (Implementierungshandbuch für den Sentinel Identity Tracking-Treiber):** Der Sentinel Identity Tracking-Treiber (Treiber für Identitätsüberwachung) ermöglicht die Integration mit Identity Manager und Sentinel zum Nachverfolgen von Benutzerkontoinformationen. Jedes Benutzerkonto kann mehrere Kontokennungen für jedes System in der Identity Manager-Lösung besitzen. Der Treiber verfolgt jede Kontokennung und sendet diese Informationen an Sentinel. Sentinel kann Berichte ausführen, um einzelne Kontokennungen einem bestimmten Benutzer zuzuordnen. Weitere Informationen finden Sie im *Driver for Sentinel Implementation Guide* (Implementierungshandbuch für den Treiber für Sentinel).

10.1.2 Funktionen für die Passwortverwaltung

Verbesserungen der Passwortrichtlinie

Identity Manager unterstützt nun drei neue Syntaxoptionen für die Passwortrichtlinie:

- Verwendung der Microsoft-Passwortkomplexitätsrichtlinie
- Verwendung der Passwortrichtlinie von Microsoft Server 2008
- Verwendung der Novell-Syntax

Weitere Informationen finden Sie im Abschnitt "Understanding Password Management" (Grundlegendes zur Passwortverwaltung) im *Identity Manager 4.0.2 Password Management Guide* (Handbuch zur Passwortverwaltung in Identity Manager 4.0.2).

10.1.3 Funktionen für den Rollenzuordnungsadministrator

Synchronisierung der Codezuordnung

Identity Manager 4.0.2 bietet Funktionen zur Synchronisierung der Codezuordnungstabellen zwischen dem Rollenzuordnungsadministrator und dem rollenbasierten Bereitstellungsmodul. Bei der Erstellung von Zuordnungen im Rollenzuordnungsadministrator können Sie eine Aktualisierung der Codezuordnung entweder im Rollenzordnungsadministrator oder im rollenbasierten Bereitstellungsmodul auslösen, falls die Codezuordnungen nicht übereinstimmen. Eine Aktualisierung der Rollenzuordnungen kann sehr lange dauern, wenn sie für alle Treiber und Berechtigungen ausgeführt wird. Daher haben Sie mit dem Rollenzuordnungsadministrator die Möglichkeit, eine Aktualisierung nur für die Berechtigungen auszulösen, die nicht übereinstimmen. Das rollenbasierte Bereitstellungsmodul stellt auch neue SOAP-Endpunkte zum Auslösen von Aktualisierungen der Rollenzuordnungen zur Verfügung. Weitere Informationen über die Änderungen beim Rollenzuordnungsadministrator finden Sie unter "Creating Role Resource Mappings" (Erstellen von Rollenressourcenzuordnungen) im *Novell Identity Manager Role Mapping Administrator 4.0.2 User Guide* (Benutzerhandbuch für den Rollenzuordnungsadministrator in Novell Identity Manager 4.0.2). Weitere Informationen über die neuen SOAP-Endpunkte finden Sie unter "Resource Web Service (Ressourcenwebdienst) " im *User Application: Administration Guide* (Benutzeranwendung: Administrationshandbuch).

Einstellungen zur Ressourcenerstellung für den Rollenzuordnungsadministrator

Der Rollenzuordnungsadministrator stellt nun verschiedene Einstellungen für die Ressourcenerstellung bereit, mit denen Sie dem Treibernamen und dem Namen des logischen Systems beim Erstellen von Ressourcen ein Präfix hinzufügen können. Die Einstellungen zur Ressourcenerstellung ermöglichen es Ihnen auch, eine Ressourcenkategorie für automatisch erstellte Ressourcen auszuwählen. Weitere Informationen finden Sie unter "Customizing the Resource Names" (Anpassen der Ressourcennamen) im *Novell Identity Manager Role Mapping Administrator 4.0.2 User Guide* (Benutzerhandbuch für den Rollenzuordnungsadministrator in Novell Identity Manager 4.0.2).

10.1.4 Funktionen des rollenbasierten Provisioning-Moduls

Genehmigungsverfahren für den Rollenentzug

Das rollenbasierte Bereitstellungsmodul unterstützt nun die Anwendung von Genehmigungsverfahren für den Rollenentzug. Das Genehmigungsverfahren für Rollenentzugsanforderungen sowie die Liste der Genehmiger entsprechen der Vorgehensweise bei der Rollenerteilung. Wenn Sie angegeben haben, dass das Genehmigungsverfahren entsprechend der Standarddefinition der Rollenzuweisungsgenehmigung ausgeführt werden soll, dann wird dieses Verfahren angewendet. Alternativ können Sie ein benutzerdefiniertes Genehmigungsverfahren sowohl für Rollenerteilungsanforderungen als auch für Rollenentzugsanforderungen angeben. Weitere Informationen finden Sie unter "Defining the Approval Process for a Role" (Definieren des Genehmigungsprozesses für eine Rolle) im *User Application: User Guide* (Benutzeranwendung: Benutzerhandbuch).

Optimierung der Rollenlöschvorgänge

Das rollenbasierte Bereitstellungsmodul hat den Prozess der Löschung von Rollen optimiert. Wenn Sie der Benutzeranwendung die Anweisung geben, eine Rolle zu löschen, wird zunächst der Rollenstatus auf „Anstehende Löschung" festgelegt. Der Rollen- und Ressourcendienst-Treiber erkennt anschließend die Statusänderung und führt die folgenden Schritte aus:

1. Entfernt die Ressourcenzuweisungen für die Rolle.
2. Löscht die Rolle.

Weitere Informationen finden Sie unter "Deleting Roles (Löschen von Rollen) " im *User Application: User Guide* (Benutzeranwendung: Benutzerhandbuch).

SAML-Unterstützung für 64-Bit-Plattformen

SAML-Unterstützung für Single Sign-On wurde für 64-Bit-Linux- und -Windows-Plattformen hinzugefügt Weitere Informationen finden Sie unter "Single Sign On (SSO) Configuration" (SSO-Konfiguration) im *User Application: Administration Guide* (Benutzeranwendung: Benutzerhandbuch).

10.1.5 Funktionen für das Identitätsberichterstellungsmodul

Unterstützung für EAS unter Red Hat Enterprise Linux

Der Event Auditing Service (EAS) wird nun unter Red Hat Enterprise Linux 5.7 und 6.0 (32-Bit und 64-Bit) ausgeführt.

Neuer Rollenhierarchiebericht

Der Rollenhierarchiebericht wurde dem Identitätsberichterstellungsmodul hinzugefügt. In diesem Bericht werden die Inhalte der Rollenhierarchie angezeigt sowie die mit den einzelnen Rollen verknüpften Ressourcen. Weitere Informationen finden Sie im "Role Hierarchy Report" (Rollenhierarchiebericht) unter *Using Identity Manager 4.0.2 Reports* (Verwenden von Identity Manager 4.0.2-Berichten).

Möglichkeit zum Entfernen historischer Daten aus der Berichterstellungsdatenbank

Mit dem Identitätsberichterstellungsmodul können Sie nun historische Daten aus der Berichterstellungsdatenbank entfernen. Wenn das Berichterstellungsmodul einen Vorgang zum Entfernen von Daten durchführt, werden nur die Daten aus Verlaufstabellen entfernt, die älter sind als der angegebene Aufbewahrungswert. Alle Verlaufsdaten, die jünger sind als die erlaubten Aufbewahrungsintervalle, werden weiterhin aufbewahrt. Der Vorgang zum Entfernen der Daten entfernt keine aktuellen Daten. Weitere Informationen finden Sie unter "Configuring Settings and Data Collection" (Konfigurieren von Einstellungen und Datensammlung) im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul).

10.1.6 Designer-Funktionen

REST-Aktivitätsunterstützung für Workflows

Designer 4.0.2 verfügt jetzt über eine neue Aktivität im Provisioning Request Definition-Editor (Provisioning-Anforderungsdefinitions-Editor), die es Benutzern ermöglicht, beim Verarbeiten von Workflowdaten REST-Endpunkte oder -Ressourcen aufzurufen. Mithilfe der REST-Aktivität können Workflows Daten mit REST-Diensten in und außerhalb der Organisation austauschen, und Benutzer können von einem REST-Dienst empfangene Daten als Entscheidungshilfe in Genehmigungsformularen verwenden.

Weitere Informationen finden Sie im Abschnitt "Rest Activity" (REST-Aktivität) im *User Application: Design Guide* (Benutzeranwendung: Entwurfshandbuch).

Verbesserungen bei der Integrations-Aktivität für Workflows

Designer 4.0.2 enthält verschiedene Verbesserungen an der Integrations-Aktivität im Provisioning Request Definition-Editor, wie das Auflösen von Animationsfehlern und das Reduzieren der Größe bereitgestellter PRDs. Außerdem können Benutzer jetzt mithilfe der Integrations-Aktivität SOAP-Anforderungen für die Aktivität in der Designer-Benutzeroberfläche leichter generieren.

Weitere Informationen finden Sie im Abschnitt "Adding an Integration Activity" (Hinzufügen einer Integrations-Aktivität) im *User Application: Design Guide* (Benutzeranwendung: Entwurfshandbuch).

Leistungsverbesserungen in Designer

Designer 4.0.2 verfügt über verschiedene Verbesserungen bei der Leistung. Dazu gehören eine bessere Leistung beim Verwenden der verschiedenen im Produkt enthaltenen Editoren, eine verbesserte Darstellung der Konfigurationsseiten in der Benutzeroberfläche, eine höhere Geschwindigkeit von Project Checker sowie gelöste Speicherprobleme. Für weitere Informationen öffnen Sie Designer 4.0.2, und klicken Sie in der Symbolleiste auf *Help* > *What's New* (Hilfe > Neuigkeiten).

Designer-Optimierung für optionalen Import von Rollen und Ressourcen

Beim Konfigurieren eines Projekts in Designer war es bisher erforderlich, dass automatisch eine große Anzahl von Rollen und Ressourcen aus dem Identitätsdepot importiert werden musste. Jetzt kann Designer vom Benutzer so konfiguriert werden, dass der Rollenkatalog nicht mehr automatisch importiert werden soll. Wenn ein Benutzer nicht möchte, dass Rollen oder Ressourcen importiert

werden, kann er die Option *Do not import role catalog (excluding system roles)* (Rollenkatalog nicht importieren (außer Systemrollen)) auf der Seite *Novell* > *Provisioning* > *Import/Deploy* (Novell > Provisioning > Importieren/Bereitstellen) in den Designer-Voreinstellungen deaktivieren. Der Rollenkatalog wird dann nicht automatisch in Designer importiert, wodurch die Benutzer Zeit sparen und diese Rollen und Ressourcen in Designer auch nicht verwalten müssen.

Weitere Informationen finden Sie im Abschnitt "Configuring Roles" (Konfigurieren von Rollen) im *User Application: Design Guide* (Benutzeranwendung: Entwurfshandbuch).

Entfernen nicht verwendeter Pakete aus dem Paketkatalog in Designer

Wenn ein Benutzer über eine große Anzahl nicht benötigter Pakete verfügt, die in den Paketkatalog importiert wurden, bietet Designer 4.0.2 die Möglichkeit an, nicht verwendete Pakete aus dem Katalog zu löschen. Dabei werden sämtliche importierten Pakete, die nicht in einem Treiber, Treibersatz oder Identitätsdepot installiert sind, aus dem Projekt entfernt.

Weitere Informationen finden Sie im Abschnitt "Removing Packages from the Package Catalog" (Entfernen von Paketen aus dem Paketkatalog) im *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide* (Adminstrationshandbuch für Designer 4.0.2 for Identity Manager 4.0.2).

10.1.7 Analyzer-Funktionen

Leistungsverbesserungen in Analyzer

Analyzer 4.0.2 bietet eine bessere Leistung durch Verwendung der Batching-Funktion beim MySQL-Datenbankserver. Analyzer kann jetzt eine Million Datensätze auf einmal in die Analyzer-Datenbank importieren. Weitere Informationen finden Sie unter "Database Settings" (Datenbankeinstellungen) im *Analyzer 4.0.2 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.2 für Identity Manager).

10.2 Neuerungen in Identity Manager 4.0.1

- Abschnitt 10.2.1, „Identity Manager Advanced Edition im Vergleich zur Standard Edition“, auf Seite 97
- Abschnitt 10.2.2, „Telemetrie“, auf Seite 98
- Abschnitt 10.2.3, „Aktivität „Ressourcenanforderung““, auf Seite 98
- Abschnitt 10.2.4, „Neue Berichte für das Identitätsberichterstellungsmodul“, auf Seite 98
- Abschnitt 10.2.5, „Anwendungen, die zur Designer-Palette hinzugefügt wurden“, auf Seite 98

10.2.1 Identity Manager Advanced Edition im Vergleich zur Standard Edition

Um den verschiedenen Anforderungen der Kunden gerecht zu werden, wird Identity Manager 4.0.1 in zwei Versionen ausgeliefert, Advanced Edition und Standard Edition. Die Advanced Edition enthält einen vollständigen Satz an Funktionen der Unternehmensklasse zur Bereitstellung von Benutzern. Die Standard Edition enthält nur einen Teil der Funktionen, die in der Identity Manager Advanced Edition verfügbar sind, bietet aber weiterhin alle Funktionen der älteren Versionen von Identity Manager. Eine Gegenüberstellung der Funktionen der Advanced und der Standard Edition von Identity Manager finden Sie im Versionenvergleich zu Identity Manager (http://www.novell.com/products/identitymanager/features/identitymanager-version-comparison.html).

10.2.2 Telemetrie

Identity Manager Telemetry ist ein neuer Auftrag, der in Identity Manager 4.0.1 eingeführt wurde. Der Auftrag kann als Zählprogramm für die Lizenznutzung und als Lizenzüberwachungswerkzeug eingesetzt werden. Mithilfe des Lizenzüberwachungswerkzeugs können Identity Manager-Kunden mehr Lizenzen hinzufügen oder nicht verwendete Lizenzen deaktivieren. Die Kunden können auch von Vorteilen wie z. B. der Preisgebung für inaktive Benutzer profitieren.

10.2.3 Aktivität „Ressourcenanforderung“

Die Aktivität „Ressourcenanforderung“ ermöglicht Ihnen, das Zuweisen bzw. Entziehen von Ressourcen zu automatisieren. Beispielsweise können Sie eine Bereitstellungsanforderungsdefinition schreiben, die einem neuen Mitarbeiter an seinem ersten Arbeitstag alle benötigten Ressourcen bereitstellt. Mithilfe der Aktivität „Ressourcenanforderung“ können Sie die Genehmigung von bestimmten Ressourcen für diesen Mitarbeiter automatisieren. Ausführliche Informationen zur Aktivität „Ressourcenanforderung“ finden Sie unter „*Resource Request Activity*“ (Aktivität „Ressourcenanforderung“) im *User Application: Design Guide* (Designhandbuch zur Benutzeranwendung).

10.2.4 Neue Berichte für das Identitätsberichterstellungsmodul

Folgende Berichte wurden hinzugefügt:

- **Benutzerstatusänderung im Identitätsdepot:** Enthält für die Identitätsdepotbenutzer signifikante Ereignisse.
- **Benutzerpasswortänderung im Identitätsdepot:** Zeigt alle Benutzerpasswortänderungen im Identitätsdepot an.
- **Zugriffsanfragen nach Empfänger:** Enthält die Workflow-Prozesse zu Ressourcenzuweisungen gruppiert nach Empfänger.
- **Zugriffsanfragen nach Anforderer:** Enthält die Workflow-Prozesse zu Ressourcenzuweisungen gruppiert nach Anforderer.
- **Zugriffsanfragen nach Ressource:** Enthält die Workflow-Prozesse zu Ressourcenzuweisungen gruppiert nach Ressourcen.

Weitere Informationen zu neuen Berichten finden Sie im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul).

10.2.5 Anwendungen, die zur Designer-Palette hinzugefügt wurden

Folgende Anwendungen wurden zur Designer-Palette hinzugefügt:

- Schwarzes Brett
- Google-Apps
- RSA

10.3 Neuerungen in Identity Manager 4.0

- Abschnitt 10.3.1, „Identitätsberichterstellungsmodul“, auf Seite 99
- Abschnitt 10.3.2, „Neue Treiber“, auf Seite 99

- Abschnitt 10.3.3, „Unterstützung für XDAS-Revisionen“, auf Seite 100
- Abschnitt 10.3.4, „Pakete ersetzen Treiberkonfigurationsdateien“, auf Seite 100
- Abschnitt 10.3.5, „Rollenzuordnungsadministrator“, auf Seite 100
- Abschnitt 10.3.6, „Analyzer“, auf Seite 100
- Abschnitt 10.3.7, „Integriertes Installationsprogramm“, auf Seite 100

10.3.1 Identitätsberichterstellungsmodul

Mit dem Identity-Berichterstellungsmodul können Sie Berichte generieren, die Informationen zu verschiedenen Aspekten Ihrer Identity Manager-Konfiguration liefern, einschließlich erfasster Informationen zu einem oder mehreren Identitätsdepots oder verwalteten Systemen. Das Berichterstellungsmodul enthält eine Reihe von vordefinierten Berichtsdefinitionen, die Sie zum Generieren von Berichten verwenden können. Zusätzlich haben Sie die Möglichkeit, benutzerdefinierte Berichte zu importieren, die in einem Drittanbieter-Werkzeug definiert sind.

Für das Identitätsberichterstellungsmodul sind zwei neue Service-Treiber erforderlich:

- Datenerfassungsdiensttreiber
- Treiber „Verwaltetes System - Gateway“

Nähere Informationen zum Berichterstellungsmodul und zu den beiden Berichterstellungstreibern finden Sie im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul). Nähere Informationen zu den vordefinierten Berichten finden Sie unter *Verwenden von Identity Manager 4.0.2 Berichten*.

10.3.2 Neue Treiber

Die folgenden neuen Treiber sind in Identity Manager 4.0 enthalten:

- „SharePoint-Treiber (.NET Remote Loader)“, auf Seite 99
- „Salesforce.com-Treiber“, auf Seite 99

SharePoint-Treiber (.NET Remote Loader)

Der SharePoint-Treiber für Novell Identity Manager ermöglicht das Synchronisieren von Benutzer- und Gruppenmitgliedschaftsereignissen zwischen dem Identitätsdepot und einer SharePoint 2007- oder SharePoint 2010-Site-Sammlung. Ein einzelner Treiber kann diese Ereignisse für eine einzelne Site-Sammlung verarbeiten, die Benutzer- und Gruppenmitgliedschaftsinformationen für einen oder mehrere SharePoint-Sites enthält. Weitere Informationen hierzu finden Sie im *Identity Manager 4.0.2 Driver for SharePoint Implementation Guide* (Implementierungshandbuch für Identity Manager 4.0-Treiber für SharePoint).

Salesforce.com-Treiber

Identity Manager 4.0 bietet die automatische Bereitstellung und Synchronisierung von Benutzern mit Cloud-Anwendungen. Der neue Salesforce.com-Treiber für Novell Identity Manager kann Benutzer nahtlos für eine Salesforce.com-Cloud-Anwendung bereitstellen bzw. die Bereitstellung aufheben. So ist sichergestellt, dass Benutzeridentitätsinformationen zwischen dem Identitätsdepot und der Cloud-Anwendung einheitlich sind. Der Salesforce.com-Treiber unterstützt darüber hinaus die sichere Passwortsynchronisierung zwischen Identitätsdepot und Salesforce.com-Cloud sowie einen

authentifizierten Proxyserver und konfigurierbare Benutzerprofile für die automatische Benutzerbereitstellung. Weitere Informationen hierzu finden Sie im *Identity Manager 4.0.2 Driver for Salesforce.com Implementation Guide* (Implementierungshandbuch für Identity Manager 4.0-Treiber für Salesforce.com).

10.3.3 Unterstützung für XDAS-Revisionen

Identity Manager 4.0 unterstützt XDAS-basierte Revisionen, die die Revisionsfunktionalität des Novell Audit-Plattformagenten erweitert. Es verwendet ein gemeinsames XDAS-Schema für Identity Manager, NMAS, eDirectory und den Rollenzuordnungsadministrator. Der neue Revisionsdienst unterstützt außerdem die syslog- und Datei-Appender. Weitere Informationen finden Sie im *Handbuch zum Identitätsberichterstellungsmodul* und im *Identity Manager 4.0.2 Berichterstellungshandbuch für Novell Sentinel*.

10.3.4 Pakete ersetzen Treiberkonfigurationsdateien

Identity Manager 4.0 arbeitet mit Paketen, die hochwertige Bausteine von Identity Manager-Richtlinieninhalten enthalten. Anstelle von Treiberkonfigurationsdateien werden jetzt Pakete zum Erstellen von Treibern verwendet. Weitere Informationen finden Sie unter "Verwalten von Paketen" im *Administrationshandbuch zu Designer 4.0.2 für Identity Manager 4.0.2*.

10.3.5 Rollenzuordnungsadministrator

Der Rollenzuordnungsadministrator ist ein neues Werkzeug zum Analysieren und Erteilen von Autorisierungen oder Berechtigungen, die in Ihren IT-Systemen gewährt werden können. Die Autorisierungen und Berechtigungen können auch von einem Geschäftsanalysten und nicht nur von IT-Mitarbeitern oder Beratern erteilt werden. Weitere Informationen finden Sie im *Benutzerhandbuch zum Novell Identity Manager-Rollenzuordnungsadministrator 4.0.2*.

10.3.6 Analyzer

Mithilfe von Analyzer können Sie Identitätsdaten für die Verwaltung mit Identity Manager diagnostizieren, bereinigen und vorbereiten. Weitere Informationen hierzu finden Sie im *Analyzer 4.0.2 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.1 für Identity Manager).

10.3.7 Integriertes Installationsprogramm

Identity Manager 4.0 verfügt über ein integriertes Installationsprogramm, das alle Identity Manager-Komponenten installiert und konfiguriert. Das Installationsprogramm wird für neue Installationen in kleinen und mittelgroßen Umgebungen verwendet. Weitere Informationen finden Sie im *Identity Manager 4.0.2 Integrated Installation Guide* (Handbuch zur integrierten Installation von Identity Manager 4.0).

III Aufrüsten von Identity Manager

Verwenden Sie zum Aufrüsten von Identity Manager-Komponenten die individuellen Produktinstallationsprogramme für die Aufrüstung auf Identity Manager 4.0.2. Für die Aufrüstung von der Identity Manager 4.0.2 Standard Edition auf die Advanced Edition gibt es ein anderes Verfahren, das nur Konfigurationsänderungen beinhaltet. Für diese Aufrüstung müssen Sie nicht das Identity Manager-Installationsprogramm ausführen. Weitere Informationen zur Aufrüstung von Identity Manager finden Sie im Abschnitt "Aufrüsten" im *Identity Manager 4.0.2 Aufrüstungs- und Migrationshandbuch*.

11 Aufrüstung im Vergleich zu Migration

Informieren Sie sich vor dem Beginn über die Unterschiede zwischen einer Aufrüstung und einer Migration. Informationen hierzu finden Sie unter “Aufrüsten oder Migrieren” im *Identity Manager 4.0.2 Aufrüstungs- und Migrationshandbuch*.

IV Deinstallation von Identity Manager

Wenn Sie Identity Manager deinstallieren möchten, müssen Sie jede Komponente deinstallieren.

- Kapitel 12, „Deinstallation der Identity Manager-Komponenten“, auf Seite 107

12 Deinstallation der Identity Manager-Komponenten

Deinstallieren Sie die Identity Manager-Komponenten in der angegebenen Reihenfolge.

- Abschnitt 12.1, „Entfernen von Objekten aus eDirectory“, auf Seite 107
- Abschnitt 12.2, „Deinstallation des Metaverzeichnis-Servers“, auf Seite 108
- Abschnitt 12.3, „Deinstallieren von Remote Loader“, auf Seite 109
- Abschnitt 12.4, „Deinstallation des rollenbasierten Bereitstellungsmoduls“, auf Seite 109
- Abschnitt 12.5, „Deinstallation der Komponenten des Identitätsberichterstellungsmoduls“, auf Seite 111
- Abschnitt 12.6, „Deinstallieren von iManager“, auf Seite 112
- Abschnitt 12.7, „Deinstallieren von eDirectory“, auf Seite 112
- Abschnitt 12.8, „Deinstallation von Analyzer“, auf Seite 114
- Abschnitt 12.9, „Deinstallation von Designer“, auf Seite 114
- Abschnitt 12.10, „Deinstallation des Rollenzuordnungsadministrators“, auf Seite 114

12.1 Entfernen von Objekten aus eDirectory

Im ersten Schritt der Deinstallation von Identity Manager müssen alle Identity Manager-Objekte aus dem Identitätsdepot gelöscht werden. Wenn es sich bei einem der Treibersatzobjekte um Stammobjekte der Partition in eDirectory handelt, muss die Partition mit der übergeordneten Partition zusammengeführt werden, bevor das Treibersatzobjekt gelöscht werden kann. Wenn der Treibersatz erstellt wird, fordert Sie der Assistent dazu auf, eine eigene Partition für den Treibersatz zu erstellen.

1. Führen Sie eine Zustandsüberprüfung der eDirectory-Datenbank aus. Falls Fehler auftreten, beheben Sie diese, bevor Sie fortfahren.

   Weitere Informationen hierzu finden Sie unter Keeping eDirectory Healthy (http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html) (Funktionsfähigkeit von eDirectory aufrechterhalten) im *Administrationshandbuch zu Novell eDirectory 8.8*.
2. Melden Sie sich bei iManager als Administrator mit vollständigen Berechtigungen für die eDirectory-Baumstruktur an.
3. Wählen Sie für Partitionen und Reproduktionen die Option zum Zusammenführen von Partitionen aus.
4. Wechseln Sie zum Treibersatzobjekt, das das root-Objekt der Partition ist, und markieren Sie es. Klicken Sie anschließend auf *OK*.
5. Warten Sie, bis der Zusammenführungsprozess abgeschlossen ist, und klicken Sie anschließend auf *OK*.

6 Löschen Sie das Treibersatzobjekt.

   Wenn Sie das Treibersatzobjekt löschen, werden alle mit diesem Treibersatz verknüpften Treiberobjekte gelöscht.

7 Wiederholen Sie Schritt 3 bis Schritt 6 für alle Treibersatzobjekte in der eDirectory-Datenbank, bis alle gelöscht wurden.

8 Wiederholen Sie Schritt 1, um sicherzustellen, dass alle Zusammenführungen abgeschlossen sind und alle Objekte gelöscht wurden.

12.2 Deinstallation des Metaverzeichnis-Servers

Wenn Identity Manager installiert ist, wird ein Deinstallationsskript auf dem Identity Manager-Server abgelegt. Mithilfe dieses Skripts können Sie alle Services, Pakete und Verzeichnisse entfernen, die bei der Installation von Identity Manager erstellt wurden.

- Abschnitt 12.2.1, „Deinstallation unter Linux/UNIX“, auf Seite 108
- Abschnitt 12.2.2, „Deinstallieren einer Nicht-root-Installation“, auf Seite 108
- Abschnitt 12.2.3, „Deinstallation unter Windows“, auf Seite 108

12.2.1 Deinstallation unter Linux/UNIX

Führen Sie zur Deinstallation von Identity Manager unter Linux/UNIX das Deinstallationsskript aus, das sich unter `/root/idm/Uninstall_Identity_Manager/Uninstall_Identity_Manager` befindet. Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./Uninstall_Identity_Manager`.

12.2.2 Deinstallieren einer Nicht-root-Installation

Wenn Identity Manager von einem Nicht-`root`-Benutzer installiert wurde, wird das `idm`-Verzeichnis in das Verzeichnis des Benutzers gestellt, der Identity Manager installiert hat.

Wenn Sie eine Nicht-root-Installation von Identity Manager deinstallieren möchten, müssen Sie das Deinstallationsskript als der Benutzer ausführen, der Identity Manager installiert hat. Es befindet sich unter `/eDirectory_Stammverzeichnis/opt/novell/eDirectory/bin/idm-uninstall`.

Das Skript bereinigt die Benutzer-RPM-Datenbank, die während der Installation von Identity Manager erstellt wurde.

12.2.3 Deinstallation unter Windows

Die Schritte zum Deinstallieren des Metaverzeichnis-Servers sind bei allen unterstützten Windows-Plattformen unterschiedlich.

- **Windows 2003 SP2 (32 Bit und 64 Bit):** Wählen Sie in der Systemsteuerung *Software* > *Identity Manager* und dann *Ändern/Entfernen*.
- **Windows 2008 SP1 (32 Bit und 64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Identity Manager*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.
- **Windows 2008 R2 (64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Identity Manager*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.

12.3 Deinstallieren von Remote Loader

Wenn Remote Loader installiert ist, wird ein Deinstallationsskript auf dem Remote Loader-Server abgelegt. Mithilfe des Skripts können Sie alle Services, Pakete und Verzeichnisse entfernen, die bei der Installation von Remote Loader erstellt wurden.

- Abschnitt 12.3.1, „Deinstallation unter Linux/UNIX“, auf Seite 109
- Abschnitt 12.3.2, „Deinstallation unter Windows“, auf Seite 109

12.3.1 Deinstallation unter Linux/UNIX

Führen Sie zur Deinstallation von Remote Loader unter Linux/UNIX das Deinstallationsskript aus, das sich unter `/root/idm/Uninstall_Identity_Manager/Uninstall_Identity_Manager` befindet. Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./Uninstall_Identity_Manager`.

Wenn Remote Loader von einem Nicht-`root`-Benutzer installiert wurde, wird das `idm`-Verzeichnis in das Verzeichnis des Benutzers gestellt, der Remote Loader installiert hat.

12.3.2 Deinstallation unter Windows

Die Schritte zum Deinstallieren von Remote Loader sind bei allen unterstützten Windows-Plattformen unterschiedlich.

- **Windows 2003 SP2 (32 Bit und 64 Bit):** Wählen Sie in der Systemsteuerung *Software* > *Identity Manager* und dann *Ändern/Entfernen*.
- **Windows 2008 SP1 (32 Bit und 64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Identity Manager*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.
- **Windows 2008 R2 (64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Identity Manager*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.

12.4 Deinstallation des rollenbasierten Bereitstellungsmoduls

Das rollenbasierte Bereitstellungsmodul umfasst mehrere Komponenten, die alle einzeln deinstalliert werden müssen.

- Abschnitt 12.4.1, „Löschen der Treiber“, auf Seite 109
- Abschnitt 12.4.2, „Deinstallation der Benutzeranwendung“, auf Seite 110
- Abschnitt 12.4.3, „Deinstallation des Anwendungsservers und der Datenbank“, auf Seite 110

12.4.1 Löschen der Treiber

Sie müssen den Benutzeranwendungstreiber und den Rollen- und Ressourcenservice-Treiber löschen.

1 Halten Sie den Benutzeranwendungstreiber, den Rollen- und den Ressourcenservice-Treiber an.

- **Designer:** Klicken Sie mit der rechten Maustaste auf die Treiberzeile und klicken Sie anschließend auf *Live* > *Treiber anhalten*.
- **iManager:** Klicken Sie auf der Seite „Treibersatz-Überblick“ auf die obere rechte Ecke des Treibers und dann auf *Treiber anhalten*.

2 Löschen Sie den Benutzeranwendungstreiber und den Rollen- und Ressourcenservice-Treiber.

- **Designer:** Klicken Sie mit der rechten Maustaste auf die Treiberzeile und wählen Sie *Löschen*.
- **iManager:** Klicken Sie auf der Seite „Treibersatz-Überblick“ auf *Treiber* > *Treiber löschen* und dann auf den zu löschenden Treiber.

12.4.2 Deinstallation der Benutzeranwendung

- **Linux/UNIX:** Führen Sie das Deinstallationsskript aus, das sich unter `/root/Roles_Based_Provisioning_Module_for_Novell_Identity_Manager/Uninstall Roles Based Provisioning Module for Novell Identity Manager` befindet.

  Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./Uninstall\ Roles\ Based\ Provisioning\ Module\ for\ Novell\ Identity\ Manager`.
- **Windows:** Die Schritte zum Deinstallieren der Benutzeranwendung sind bei allen unterstützten Windows-Plattformen unterschiedlich.
  - **Windows 2003 SP2 (32 Bit und 64 Bit):** Wählen Sie in der Systemsteuerung *Software* > *Rollenbasiertes Bereitstellungsmodul* und klicken Sie dann auf *Ändern/Entfernen*.
  - **Windows 2008 SP1 (32 Bit und 64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Rollenbasiertes Bereitstellungsmodul*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.
  - **Windows 2008 R2 (64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Rollenbasiertes Bereitstellungsmodul*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.

12.4.3 Deinstallation des Anwendungsservers und der Datenbank

Die Benutzeranwendung wird auf folgenden Anwendungsservern und Datenbanken ausgeführt.

Tabelle 12-1 *Unterstützte Anwendungsserver und Datenbanken*

Anwendungsserver	Datenbank
JBoss 5.1.0	◆ MS SQL 2008 ◆ MySQL Version 5.1 ◆ Oracle 11g ◆ PostgreSQL 8.4.3 und 9
WebSphere 7.0	◆ DB2 9.5b ◆ MS SQL 2008 ◆ Oracle 11g ◆ PostgreSQL 8.4.3 und 9
WebLogic 10.3	◆ MS SQL 2008 ◆ Oracle 11g ◆ PostgreSQL 8.4.3 und 9

Im Folgenden wird beschrieben, wie JBoss und PostgreSQL deinstalliert werden. Wenn Sie einen anderen Anwendungsserver und eine andere Datenbank verwenden, ziehen Sie die Dokumentation für diese Produkte zu Rate.

- **Linux/UNIX:** Führen Sie das Deinstallationsskript aus, das sich unter `/opt/novell/idm/Postgres/JBossPostgreSQL_Uninstaller/JBossPostgreSQL_deinstallieren` befindet.

  Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./Uninstall_JBossPostgreSQL`.
- **Windows:** Die Schritte zum Deinstallieren von JBoss und PostgreSQL sind bei allen unterstützten Windows-Plattformen unterschiedlich.
  - **Windows 2003 SP2 (32 Bit und 64 Bit):** Wählen Sie in der Systemsteuerung *Software* > *JBossPostgreSQL* und dann *Ändern/Entfernen*.
  - **Windows 2008 SP1 (32 Bit und 64 Bit):** Klicken Sie auf *Programme und Funktionen* > *JBossPostgreSQL*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.
  - **Windows 2008 R2 (64 Bit):** Klicken Sie auf *Programme und Funktionen* > *JBossPostgreSQL*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.

12.5 Deinstallation der Komponenten des Identitätsberichterstellungsmoduls

Das Identitätsberichterstellungsmodul besteht aus mehreren Komponenten. Zum Deinstallieren des Identitätsberichterstellungsmoduls muss jede Komponente einzeln deinstalliert werden.

- Abschnitt 12.5.1, „Löschen der Berichterstellungstreiber“, auf Seite 111
- Abschnitt 12.5.2, „Deinstallation des Identity-Berichterstellungsmoduls“, auf Seite 111
- Abschnitt 12.5.3, „Deinstallation des Event Auditing Service“, auf Seite 112

12.5.1 Löschen der Berichterstellungstreiber

Sie müssen den Datenerfassungstreiber und den Treiber „Verwaltetes System - Gateway“ löschen.

1. Halten Sie den Datenerfassungstreiber und den Treiber „Verwaltetes System - Gateway“ an.
   - **Designer:** Klicken Sie mit der rechten Maustaste auf die Treiberzeile und klicken Sie anschließend auf *Live* > *Treiber anhalten*.
   - **iManager:** Klicken Sie auf der Seite „Treibersatz-Überblick“ auf die obere rechte Ecke des Treibers und dann auf *Treiber anhalten*.
2. Löschen Sie den Datenerfassungstreiber und den Treiber „Verwaltetes System - Gateway“.
   - **Designer:** Klicken Sie mit der rechten Maustaste auf die Treiberzeile und wählen Sie *Löschen*.
   - **iManager:** Klicken Sie auf der Seite „Treibersatz-Überblick“ auf *Treiber* > *Treiber löschen* und dann auf den zu löschenden Treiber.

12.5.2 Deinstallation des Identity-Berichterstellungsmoduls

- **Linux:** Führen Sie das Deinstallationsskript aus, das sich unter `/opt/novell/IdentityReporting/Uninstall_Identity Reporting` befindet.

Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./Uninstall\ Identity\ Reporting`.

- **Windows:** Die Schritte zum Deinstallieren des Identitätsberichterstellungsmodul sind bei allen unterstützten Windows-Plattformen unterschiedlich.
  - **Windows 2003 SP2 (32 Bit und 64 Bit):** Wählen Sie in der Systemsteuerung *Software* > *Identitätsberichterstellung* und dann *Ändern/Entfernen*.
  - **Windows 2008 SP1 (32 Bit und 64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Identitätsberichterstellung*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.
  - **Windows 2008 R2 (64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Identitätsberichterstellung*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.

12.5.3 Deinstallation des Event Auditing Service

Der Event Auditing Service (EAS) wird nur auf SLES-Plattformen unterstützt. Führen Sie das Deinstallationsskript aus, das sich unter `/opt/novell/sentinel_eas/Uninstall_Event Auditing Service/Uninstall Event Auditing Service` befindet. Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./Uninstall\ Event\ Auditing\ Service`.

12.6 Deinstallieren von iManager

- **Linux:** Führen Sie als `root`-Benutzer das Deinstallationsskript aus, das sich unter `/var/opt/novell/iManager/nps/UninstallerData/UninstalliManager` befindet.

  Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./UninstalliManager`.
- **Windows:** Die Schritte zum Deinstallieren von iManager sind bei allen unterstützten Windows-Plattformen unterschiedlich.
  - **Windows 2003 SP2 (32 Bit und 64 Bit):** Wählen Sie in der Systemsteuerung *Software* > *Novell iManager* und dann *Ändern/Entfernen*.
  - **Windows 2008 SP1 (32 Bit und 64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Novell iManager*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.
  - **Windows 2008 R2 (64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Novell iManager*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.

  Tomcat und NICI sind in der Systemsteuerung separat aufgeführt. Wenn Sie die Programme nicht mehr verwenden, können Sie sie separat deinstallieren. Wenn eDirectory auf demselben Server installiert ist, wird NICI benötigt, damit eDirectory weiterhin ausgeführt werden kann. Wenn Sie eDirectory nicht deinstallieren, deinstallieren Sie auch NICI nicht.

12.7 Deinstallieren von eDirectory

Bevor Sie eDirectory deinstallieren, müssen Sie Ihre eDirectory-Baumstruktur und die Reproduktionsplatzierungen kennen, damit keine Probleme im eDirectory-Baum entstehen.

Beantworten Sie folgende Fragen, bevor Sie eDirectory deinstallieren:

- ❒ Gibt es mehrere Server im Baum?

Wenn Sie dies mit „Ja“ beantworten, fahren Sie mit den anderen Fragen in dieser Liste fort. Wenn Sie dies mit „Nein“ beantworten, können Sie eDirectory entfernen.

- ❒ Sind auf diesem Server Masterreproduktionen gespeichert?

  Lautet die Antwort „Ja“, müssen Sie einen anderen Server in diesem Reproduktionsring zum Master bestimmen, bevor Sie eDirectory entfernen. Weitere Informationen finden Sie unter “Verwalten von Partitionen und Reproduktionen” (http://www.novell.com/documentation/edir88/edir88/data/a2iiiik.html) im *Administrationshandbuch zu Novell eDirectory 8.8*..

- ❒ Enthält dieser Server die einzige Kopie einer Partition?

  Lautet die Antwort „Ja“, müssen Sie diese Partition mit der übergeordneten Partition zusammenführen oder eine Reproduktion dieser Partition auf einen anderen Server kopieren und diesen zum Masterreproduktionsserver machen. Weitere Informationen finden Sie unter “Verwalten von Partitionen und Reproduktionen” (http://www.novell.com/documentation/edir88/edir88/data/a2iiiik.html) im *Administrationshandbuch zu Novell eDirectory 8.8*.

Wenn Sie sichergestellt haben, dass der eDirectory-Baum bereit ist, gehen Sie wie folgt vor, um eDirectory zu deinstallieren:

1. Wenn dies ein Baum mit nur einem Server ist, fahren Sie direkt mit Schritt 2 fort. Andernfalls führen Sie eine Zustandsüberprüfung der eDirectory-Datenbank aus. Falls Fehler auftreten, beheben Sie diese, bevor Sie fortfahren. Weitere Informationen hierzu finden Sie unter “Keeping eDirectory Healthy” (http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html) (Funktionsfähigkeit von eDirectory aufrechterhalten) im *Administrationshandbuch zu Novell eDirectory 8.8*.
2. Deinstallieren Sie eDirectory.
   - **Linux/UNIX:** Führen Sie das Deinstallationsskript aus, das sich unter `/opt/novell/eDirectory/sbin/nds-uninstall` befindet.

     Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./nds-uninstall`.
   - **Windows:** Die Schritte zum Deinstallieren von eDirectory sind bei allen unterstützten Windows-Plattformen unterschiedlich.
     - **Windows 2003 SP2 (32 Bit und 64 Bit):** Wählen Sie in der Systemsteuerung *Software* > *Novell eDirectory* und dann *Ändern/Entfernen*.
     - **Windows 2008 SP1 (32 Bit und 64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Novell eDirectory*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.
     - **Windows 2008 R2 (64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Novell eDirectory*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.
3. (Bedingt) Wenn dies ein Baum mit mehreren Servern ist, löschen Sie alle im Baum verbliebenen serverspezifischen Objekte und führen Sie eine weitere Zustandsüberprüfung durch. Hierdurch wird sichergestellt, dass der Server ordnungsgemäß aus dem Baum entfernt wurde.

   Weitere Informationen hierzu finden Sie unter “Keeping eDirectory Healthy” (http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html) (Funktionsfähigkeit von eDirectory aufrechterhalten) im *Administrationshandbuch zu Novell eDirectory 8.8*.

12.8 Deinstallation von Analyzer

1. Vergewissern Sie sich, dass Analyzer geschlossen ist.
2. So deinstallieren Sie Analyzer:
   - **Linux:** Führen Sie das Deinstallationsskript aus, das sich unter `<installation_directory>/analyzer/UninstallAnalyzer/Uninstall Analyzer for Identity Manager` befindet.

     Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./Uninstall\ Analyzer\ for\ Identity\ Manager`.
   - **Windows:** Die Schritte zum Deinstallieren von Analyzer sind bei allen unterstützten Windows-Plattformen unterschiedlich.
     - **Windows 2003 SP2 (32 Bit und 64 Bit):** Wählen Sie in der Systemsteuerung *Software* > *Analyzer für Identity Manager* und dann *Ändern/Entfernen*.
     - **Windows 2008 SP1 (32 Bit und 64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Analyzer für Identity Manager*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.
     - **Windows 2008 R2 (64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Analyzer für Identity Manager*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.

12.9 Deinstallation von Designer

1. Vergewissern Sie sich, dass Designer geschlossen ist.
2. Deinstallieren Sie Designer.:
   - **Linux/UNIX:** Führen Sie das Deinstallationsskript aus, das sich unter `<Installationsverzeichnis>/designer/UninstallDesigner/Uninstall Designer for Identity Manager` befindet.

     Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./Uninstall\ Designer\ for\ Identity\ Manager`.
   - **Windows:** Die Schritte zum Deinstallieren von Designer sind bei allen unterstützten Windows-Plattformen unterschiedlich.
     - **Windows 2003 SP2 (32 Bit und 64 Bit):** Wählen Sie in der Systemsteuerung *Software* > *Designer für Identity Manager* und dann *Ändern/Entfernen*.
     - **Windows 2008 SP1 (32 Bit und 64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Designer für Identity Manager*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.
     - **Windows 2008 R2 (64 Bit):** Klicken Sie auf *Programme und Funktionen* > *Designer für Identity Manager*. Klicken Sie dann mit der rechten Maustaste und wählen Sie *Deinstallieren*.

12.10 Deinstallation des Rollenzuordnungsadministrators

1. Wechseln Sie zum Installationsverzeichnis für den Rollenzuordnungsadministrator.

   Dieses Verzeichnis wird während der Installation festgelegt. Es kann daher bei jeder Installation verschieden sein.

2 Halten Sie über die Befehlszeile den Rollenzuordnungsadministrator an, indem Sie das `stop`-Skript ausführen.

- **Linux:** `stop.sh`

  Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./stop.sh`

- **Windows:** `stop.bat`

3 Führen Sie in der Befehlszeile das Deinstallationsskript aus.

- **Linux:** `rma-uninstall.sh [-h] [-s]`
  - `[-h]`: Ruft die Hilfe auf.
  - `[-s]`: Gibt den Automatikmodus an.

  Führen Sie das Skript aus, indem Sie folgenden Befehl eingeben: `./rma-uninstall.sh`.

- **Windows:** `rma-uninstall.bat [-h] [-s]`

4 Löschen Sie das Installationsverzeichnis.